KOREAN PATENT ABSTRACT (KR)

PUBLICATION

(51) IPC Code: G11B 20/00
(11) Publication No.: P2001-0031296 (43) Publication Date: 16 April 2001
(21) Application No.: 10-2000-7004285 (22) Application Date: 21 April 2000
(86) International Application No.: PCT/US98/22126
(86) International Application Date: 19 October 1998
(87) International Publication No.: WO 99/22372
(87) International Publication Date: 06 May 1999

(71) Applicant:
SONY ELECTRONICS, INC.

(72) Inventor:
KOMURO, Teruyoshi, et al.

(54) Title of the Invention:
A METHOD AND A SYSTEM FOR TRANSFERRING INFORMATION USING AN ENCRYPTION MODE INDICATOR

Abstract:

A method and system for transferring information using an encryption mode indicator (EMI). The present invention provides several secure information communication modes in which data (e.g., representing an audio/visual work) can be transmitted from a source device to a sink device (receiving station) in a number of secure modes. In one secure mode, EMI mode A, the information of the transmission is not allowed to be copied as a whole work; this is the highest level of copy protection. In second secure mode, EMI mode B, the information of the transmission is allowed to be copied once and once only by the sink device. In a third transmission mode, no encryption is used and free copying is availabe. Depending on which secure mode is selected between mode A and mode B, a different encryption process is used by the source device to encrypt the transmission. Further, depending on which secure mode is selected between mode A and mode B, a different decryption process is used by the sink device to decrypt the transmission. The present invention is particularly useful for transmissions between a source device and a bit stream recorder which does not have the capability to extract certain encryption information from a packet header. By using different encryption processes for each transmission mode, an unauthorized device placed between the source and the sink devices that alters the EMI code will be unable to thereafter render or record the audio/visual work because the decryption process selected will differ from the encryption process used.

공개특허특2001-0031296

(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl. [6]
G11B 20/00

(11) 공개번호 특2001-0031296
(43) 공개일자 2001년04월16일

(21) 출원번호 10-2000-7004285
(22) 출원일자 2000년04월21일
번역문제출일자 2000년04월21일
(86) 국제출원번호 PCT/US 98/22126
(87) 국제공개번호 WO 99/22372
(86) 국제출원출원일자 1998년10월19일
(87) 국제공개일자 1999년05월06일
(81) 지정국 AP ARIPO특허 : 케냐, 레소토, 말라위, 수단, 스와질랜드, 우간다,

EA 유라시아특허 : 아르메니아, 아제르바이잔, 벨라루스, 키르기즈, 카자흐스탄, 몰도바, 러시아, 타지키스탄, 투르크메니스탄,

EP 유럽특허 : 오스트리아, 벨기에, 스위스, 리히텐슈타인, 독일, 덴마크, 스페인, 프랑스, 영국, 그리스, 아일랜드, 이탈리아, 룩셈부르크, 모나코, 네덜란드, 포르투칼, 스웨덴, 핀랜드,

OA OAPI특허 : 부르키나파소, 베넹, 중앙아프리카, 콩고, 코트디브와르, 카메룬, 가봉, 기네, 말리, 모리타니, 니제르, 세네갈, 차드, 토고,

국내특허 : 알바니아, 아르메니아, 오스트리아, 오스트레일리아, 아제르바이잔, 보스니아-헤르체고비나, 바베이도스, 불가리아, 브라질, 벨라루스, 캐나다, 스위스, 리히텐슈타인, 중국, 쿠바, 체코, 독일, 덴마크, 에스토니아, 스페인, 핀랜드, 영국, 그루지야, 헝가리, 이스라엘, 아이슬란드, 일본, 케냐, 키르기즈, 북한, 대한민국, 카자흐스탄, 세인트루시아, 스리랑카, 라이베리아, 레소토, 리투아니아, 룩셈부르크, 라트비아, 몰도바, 마다가스카르, 마케도니아, 몽고, 말라위, 멕시코, 노르웨이, 뉴질랜드, 슬로베니아, 슬로바키아, 타지키스탄, 투르크메니스탄, 터어키, 트리니다드토바고, 우크라이나, 우간다, 미국, 우즈베키스탄, 베트남, 폴란드, 포르투칼, 루마니아, 러시아, 수단, 스웨덴, 싱가포르,

(30) 우선권주장 8/957,0511997년10월24일미국(US)

(71) 출원인 소니 일렉트로닉스 인코포레이티드 밀러 제리 에이
미국, 뉴저지 07656, 파크 리지, 원 소니 드라이브

(72) 발명자 코무로,테루요시
일본,카나가와216,카와사키-시,미야메-쿠,3-11-130-101,사기누마
오사와,요시토모
일본,카나가와225,요코하마-시,아오바-쿠,1-10-2-502,우쯔쿠시가오카
시마,히사토
미국,캘리포니아95070,사라토가,12610파쇼프로리스
아사노,토모유키
일본,카나가와239,요코수카-시,1-15-19-202,푸나카루

(74) 대리인 문경진
조현석

심사청구 : 없음

(54) 암호화 모드 표시기를 사용하여 정보를 전송하기 위한방법 및 시스템

요약

본 발명은 암호화 모드 표시기(EMI:encryption mode indicator)를 사용하여 정보를 전송하기 위한 방법 및 시스템에 관한 것이다. 본 발명은 데이터(예를 들어, 오디오/비주얼 저작물을 나타내는 데이터)가 다수의 안전 모드 내에서 소스 장치로부터 싱크 장치(수신 장치)로 전송될 수 있는, 여러 가지 안전 정보 통신 모드를 제공한다. 제 1 안전 모드, 즉 EMI 모드 (A)에서, 전송 정보가 전체 저작물으로써 복사되도록 허용되지 않는다; 이것은 최상위 레벨의 복사 방지이다. 제 2 안전 모드, 즉 EMI 모드 (B)에서, 전송 정보는 단지 싱크 장치에 의해서 한 번씩만 복사되도록 허용한다. 제 3 전송 모드에서는, 암호화가 사용되지 않고 자유로운 복사가 이용 가능하다. 모드 A 와 모드 B 사이에서 어떠한 안전 모드가 선택되는지에 따라, 상이한 암호화 과정이 전송을 암호화하기 위해 상기 소스 장치에 의해 이용된다. 더욱이, 모드 A 와 모드 B 사이에서 어떠한 안전 모드가 선택되는지에 따라, 상이한 해독 과정이 상기 전송을 해독하기 의해 싱크 장치에 의해 이용된다. 본 발명은 특히, 패킷 헤더로부터 특정 암호화 정보를 추출할 능력을 갖지 않는 비트 스트림 기록기 및 소스 장치 사이에서의 전송을 위해 유용하다. 각 전송 모드에 대해 서로 다른 암호화 과정을 사용하여, 소스 장치와 싱크 장치 사이에 위치되어 있고 상기 EMI 코드를 변경하는 허가받지 않은 장치는 상기 오디오/비주얼 저작물을 그에 따라 표현 또는 기록할 수 없는데, 그 이유는 선택된 해독 과정이 사용된 암호화 과정과는 다르기 때문이다.

대표도

도5a

명세서

기술분야

본 발명은 방법 및 시스템을 개시한다. 일 실시예에서, 암호화 모드 표시기를 사용하여 정보를 전송하기 위한 방법 및 시스템을 개시한다. 본 발명은 정보 통신 시스템 분야에 관한 것이다. 더욱 상세하게, 본 발명은 오디오/비주얼 저작물을 나타내는 정보를 위한 안전 통신 모드 분야에 관한 것이다.

배경기술

최근에, 다수의 오디오/비주얼(AV) 장치가 디지털 인터페이스를 사용하여 연결됨으로써 AV 정보(예를 들어, 영화, 노래 등과 같은 AV 저작물을 나타내는 정보)가 정보 소스(예를 들어, 비디오 디스크 재생기 또는 비디오 카세트 기록기)로부터 정보 디스플레이 장치(예를 들어, 텔레비전 수상기 또는 모니터) 또는 정보 싱크 장치로 전송될 수 있게 하여 주는 기술이 발전되어 왔다. 이러한 기술의 발전은 AV 장치에 대한 IEEE 1394 직렬 통신 표준의 채택을 가져왔다. 상기 IEEE 1394 직렬 통신 표준에서, 정보는 특정 헤더 정보 및 데이터 섹션을 가지는 디지털 패킷으로 전송된다.

전송된 (예를 들어, 영화를 나타내는)AV 디지털 정보는, 허가 받지 않은 사용자가 정보를 관찰하는 것과 상기 AV 저작물의 허가 받지 않은 재생 저작물을 행하는 것을 방지하기 위해, 대개는 저작권에 의해 보호받는다. 권한 부여를 받지 않은 복사를 방지하기 위해, 상기 AV 정보는 복사 제어 정보(CCI: Copy Control Information) 비트라고 불리우는 인코딩된 복사 제어 정보와 함께 전송된다. 상기 CCI 비트는 또한 복사 생성 관리 시스템(CGMS : Copy Generation Management System) 비트로써 간주될 수 있다.

인코딩된 CCI 코드는, "0", "10", 및 "11"이 각각 "무제한 복사 허용", "단일 생성 복사 허용" 및 " 복사 금지"를 나타내는 2비트로 구성된다. "1"비트 코드는 사용되지 않은 채로 남겨진다. 상기 CCI 비트가 AV 정보에 추가되는 방법은 서로 다른 종류의 AV 정보{예를 들어, MPEG(Motion Picture Expert Group), 디지털 비디오(DV) 및 오디오 데이터}에 대해 규정된다. 이러한 CCI 비트는 다운 스트림 장치에 의해 AV 정보의 사용을 제어하기 위해 상기 AV 정보를 구성하는 데이터 패킷의 데이터 부분에 추가된다.

각 데이터 기록 시간에, 기록 장치는 하나의 패킷의 AV 정보에 추가된 상기 CCI 코드를 검사하고, 만일 상기 CCI 코드가 복사 금지를 표시하면 상기 정보의 기록을 그만둔다. 만일 상기 CCI 코드가 단일 복사 허용을 나타내면, 상기 CCI 코드는 복사 금지 모드로 변화되고 그 후 상기 AV 정보는 기록 매체에서 일 회 기록된다. 그러므로, 원래의 데이터로부터 허용된 복사의 생성은 제한된다.

더욱이, 복사 생성 제한 시스템을 실행시키기 위해서, CCI 코드가 정보의 데이터 부분에서 암호화되고, 해독 정보는 상기 복사 생성 제한 시스템에 합치하는 장치만을 제조하겠다는 계약을 한 제조자에게 허가되는 방법이 채용되어 왔다. 상기 기록 장치가, 상기 AV 정보 내에서 암호화된 CCI 코드를 검사하거나 변환시키도록 하기 위해서는, 처리를 위해 상기 장치 위에 장착된 마이크로컴퓨터를 제공하거나 특수한 하드웨어를 제공하는 것이 필요하다. 다양한 종류의 AV 정보에 부합하기 위해서, 요구되는 해독 회로가 상대적으로 복잡하고 이는 장치 비용을 증가시킨다.

저렴한 기록 장치 예컨대 비트 스트림 기록(BSR:Bit Stream Recording) 장치에 있어서, 상기 장치는 위에서 언급된 특수 하드웨어가 제거됨으로 인해서 AV 정보 내에 있는 CCI코드를 판독할 수 없는 장치의 제조를 생각해 볼 수 있다. 이러한 저렴한 BSR 장치에 있어서, 복사 방지 정보를 저장하기 위해 상기 AV 패킷 내에 있는 고유 필드의 제공이 인식되어 왔다. 도 1은 패킷(CIP) 헤더(14) 섹션. 데이터 필드(16) 부분 및 IEEE 1394 표준에 따른 헤더 섹션(12)을 포함하는 종래의 정보 패킷 필드(10)를 도시한다. 상기 데

드(20)는 AV 정보가 BSR 장치로 전송될 때 이용하기 위한 복사 방지 정보를 포함한다. 비록 상기 데이터 필드(16) 섹션이 암호화된 데이터를 포함할 수 있을 지라도, 상기 CIP 헤더 섹션(14)은 일반적으로는 상기 BSR 의 제한된 용량을 수용하기 위해 암호화되지 않고 전송된다.

이러한 패킷(10)에 응답하여, 상기 BSR 장치는 상기 패킷 헤더(14)의 BCI 필드(20)를 검사하고, 만일 상기 패킷이 복사 금지를 표시하면 데이터를 기록하지 않고 만일 상기 패킷이 단일 생성 복사 허용 또는 무제한 허용을 표시하면 상기 데이터를 기록할 수 있다. 만일 허용되었다면, 패킷 헤더(14)에 저장된 BCI 코드(20)와 함께 상기 패킷 정보는 BSR 장치에 의해 기록될 수 있다. 단일 생성 복사 허용이 표시된 원래의 패킷 헤더가 제공되면, 상기 기록된 정보가 재생되어 상기 BSR 장치로부터 상기 IEEE 1394 버스로 제공될 때, 회복된 BCI 코드(20)는 복사 금지를 표시할 것이다(이미 한 번 복사되었으므로). 그러나, 만일 상기 원래의 BCI 코드가 무제한 복사를 표시하면, 상기 회복된 BCI 코드는 저장되어 전송된다.

도 2는 상기 복사 방지가 허가 받지 않은 장치(34)에 의해 손상될 수 있는 시스템(30)을 도시한다. 도시되었듯이, 소스 장치(32)는 BSR 장치인 싱크 장치(36)로 정보를 전송한다. 인터셉트 장치(34)는 이러한 통신 경로(38a 및 38b) 사이에 위치한다. 패킷이 전송 장치(32)로부터 수신 장치(36)로 전송되고 있는 동안, 패킷 헤더(14)에 있는 BCI 코드(20)는 인터셉트 장치(34)에 의해 손상될 수 있다. 예를 들어, 전송 장치(32)가 복사 금지를 표시하는 비트 코드("11")를 가지는 BCI 코드(20)를 전송하지만, 상기 BCI 코드는 전송하는 동안 단일 생성 복사 허용을 표시하는 비트 코드("10")로{장치 (34)에 의해} 변경되거나 복사 제한이 전혀 없음을 표시하는 비트 코드("0")로 변경될 수 있다. 이러한 패킷에 응답하여, 상기 데이터는 본래 복사를 금지해야 한다는 사실이 상기 BSR(36)에게 알려지지 않고, 상기 패킷 정보를 기록하는데 이는 패킷 헤더의 BCI 코드가 단일 생성 복사 또는 무제한 복사를 허용하기 때문이다. 그러므로, 상기 복사 생성은 제어 될 수 없다.

따라서, 패킷 정보가 중간 장치에 의한 손상 없이 소스 장치로부터 비지능 장치로 전송 될 수 있는 복사 방지 시스템이 필요하다. 패킷 정보가 중간 장치에 의한 손상 없이 소스 장치로부터 BSR 장치로 전송 될 수 있는 복사 방지 시스템이 더 필요하다. 전송의 복사 방지 모드 정보가 변경되는 것을 허용하지 않고, 싱크 장치에서 사용 가능한 결과를 발생시키는 시스템이 더 필요하다. 본 발명은 그러한 유리한 특징을 제공한다. 위에서 특별히 언급되지 않은 본 발명의 이러한 그리고 다른 이점은 여기에 설명된 본 발명의 논의에서 분명해질 것이다.

도면의 간단한 설명

도 1은 종래의 복사 제어 정보(CCI) 인터페이스에 따른 정보 패킷의 필드를 도시한 도면.

도 2는 소스 장치와 싱크 장치 및 그것들 사이에 결합된 허가 받지 않은 중간 장치를 구비하는 종래 시스템의 블록도.

도 3은 정보 패킷을 전달하기 위해 결합된 소스 장치와 싱크 장치를 구비하는, 본 발명에 따른 일 시스템의 블록도.

도 4는 본 발명에 따른 암호화 모드 표시기(EMI)를 포함하는 정보 패킷의 필드를 도시한 도면.

도 5a는 본 발명의 제 1 실시예에 따른 소스 장치 및 결합된 싱크 장치의 회로 블록도.

도 5b는 본 발명의 제 2 실시예에 따른 소스 장치 및 결합된 싱크 장치의 회로 블록도.

도 6a는 본 발명의 제 1 실시예의 대체 구현에 따른 비트 스트림 기록 장치의 구성 소자의 회로 블록도.

도 6b는 본 발명의 제 2 실시예의 대체 구현에 따른 비트 스트림 기록 장치
의 구성 소자의 회로 블록도.

도 7은 본 발명에 따른 소스 장치와 싱크 장치에 의해 수행되는 단계를 도시하는 흐름도.

도 8은 본 발명에 의해 지원되는 서로 다른 유형의 오디오/비주얼 장치 및 이러한 장치로의 입력 신호와 이러한 장치로부터의 출력 신호에 의해 지원된 다양한 통신 모드를 도시한 도면.

도 9는 본 발명에서의 동작 모드를 도시한 도면.

암호화 모드 표시기(EMI:Encrytion Mode Indication)를 사용하여 정보를 전송하기 위한 방법 및 시스템이 설명된다. 본 발명은 복사가 방지된 정보가 장치들 사이로 전송되고자 하는 응용 예컨대 저작권의 영향하에 있는 오디오/비주얼 저작물의 전송과 같은 응용에서 유용하다. 본 발명은 개별적인 정보 패킷을 포함하는 전송이 이루어지는 IEEE 1394 직렬 통신 표준에서 사용될 수 있다.

본 발명은 데이터(예를 들어, 오디오/비주얼 저작물을 나타내는 데이터)가 다수의 안전 모드 내에서 소스 장치로부터 싱크 장치(수신 장치)로 전송될 수 있는, 여러 가지 안전 정보 통신 모드를 제공한다. 제 1 안전 모드 즉 EMI 모드 (A)에서, 전송 정보는 전체 저작물로써 복사되도록 허용되지 않는다; 이것은 최상위 레벨의 복사 방지이다. 제 2 안전 모드 즉 EMI 모드 (B)에서, 전송 정보는 단지 싱크 장치에 의해서 한 번 씩만 복사되도록 허용한다. 제 3 전송 모드에서는, 암호화가 사용되지 않고 자유로운 복사가 이용 가능하다. 모드 (A) 와 모드 (B) 사이에서 어떠한 안전 모드가 선택되는지에 따라, 상이한 암호화 과정이 전송을 암호화하기 위해 상기 소스 장치에 의해 사용된다. 더욱이, 모드 (A) 와 모드 (B) 사이에서 어떠한 안전 모드가 선택되는지에 따라, 상이한 해독 과정이 상기 전송을 해독하기 위해 싱크 장치에 의해 이용된다. 그러므로, 상기 EMI 코드는 (1)전송의 복사 방지 모드; 및 또한 (2)사용된 암호화 과정 모두를 표시한다.

본 발명은 특히, 패킷 헤더로부터 복사 제어 정보를 추출할 능력을 갖지 않는 비트 스트림 기록기와 소스 장치 사이에서의 전송을 위해 유용하다. 각각의 전송 모드에 대해 서로 다른 암호화 과정을 사용하여, 소스 장치와 싱크 장치 사이에 위치되어 있고 상기 EMI 코드를 변경하는 허가받지 않은 장치는 상기 오디오/비주얼 저작물을 그에 따라 표현 또는 기록할 수 없는데, 그 이유는 선택된 암호화 과정이 사용된 해독 과정과는 다르기 때문이다.

본 발명의 일 실시예에서, 하나의 암호화 과정이 사용되지만 서로 다른 두 개의 암호 키(키 A 및 키 B)가 데이터를 해독하기 위해 사용된다. 이러한 실시예에서, 정보는 상기 패킷 헤더에 저장된 EMI 코드에 좌우되는 암호 키(cipher key)를 이용하여 암호화된다. 만일 상기 EMI 코드가 모드(A)에서 모드(B)로 변경되었다면, 싱크 장치는 키("B")를 이용하여 상기 전송을 해독 할 것이다. 이 예에서, 암호화는 키("A")에 의해 이루어졌기 때문에, 상기 싱크 장치에 의해 획득되는 것은 의미 없는 숫자이다. 싱크에서 회복된 것은 비록 상기 싱크 장치에 의해 기록되었을지라도, 전혀 원래의 AV 정보가 아니므로 의미가 없다.

실시예

소스 장치와 비트 스트림 기록(BSR) 장치 사이에서 복사가 방지된 정보의 안전한 전송을 제공하는 시스템 및 방법인 본 발명의 상세한 다음 설명에서, 다수의 특정 세부 항목이 본 발명의 완전한 이해를 제공하기 위해 이후에 개시된다. 그러나, 본 발명이 이러한 특정 세부 항목 또는 그것과 유사한 항목이 없이도 실행될 수 있음이 당업자에게는 이해될 것이다. 다른 예에서, 공지된 방법, 과정, 구성 소자, 및 회로가 상세하게 설명되지는 않는데 이는 불필요하게 본 발명의 논점을 흐리지 않기 위함이다.

본 발명에 따라, AV 패킷 정보는 상기 패킷 정보가 소스 장치로부터 전송되는 때에 암호화되고, 사용된 암호 모드 및 암호화 과정은 암호화 모드 표시기(EMI) 코드에 따라 변경된다. 본 발명의 EMI 코드는 세 가지 상태, 즉 복사 금지 모드, 단일 생성 복사 허용 모드 및 무제한 모드를 나타낸다. "단일 생성 복사"라는 용어는, 원래의 저작물이 그것으로부터 다수의 복사가 이루어지도록 허용할 수도 있지만 원래의 저작물(싱크 장치로 보내어진)에 대한 복사는 오직 한번만 그 자체가 복사될 수 있음을 표시한다. 선택된 암호 모드를 표시하는 상기 EMI 정보는 패킷 헤더에 저장된다. 만일 상기 EMI 정보가 수신 측에서 손상되었다면, 상기 싱크 장치(예를 들어, 수신 장치)는 상기 패킷으로부터 정확한 AV 정보를 얻을 수 없는데 이는 상기 싱크 장치가 실지 암호 모드와는 다른 암호 모드에서 해독하기 때문이다. 일실시예에서, 상기 암호 모드는 암호화 과정, 암호 키를 포함하고 레지스터의 초기 값을 포함할 수도 있다.

더욱이, 상기 전송 장치 및 상기 싱크 장치가 정보 패킷에 합해진 EMI 정보를 이해할 수 있는지에 따라, 개별적인 통신은 서로 다른 암호 모드를 이용하도록 분류될 수 있고 이에 따라 상기 전송 장치 및 싱크 장치는 다른 장치를 인식할 수 있는 것이다.

EMI 안전 통신 모드

도 3은 본 발명에서 지원되는 많은 시스템 구성에 대한 예시적인 시스템(100)을 도시한다. 시스템(100)은 디지털 프로그램을 나타내는 디지털 AV 정보를 방송 채널(115)을 통해 전달할 수 있는 선택적 무선 트랜스미터(110)를 포함한다. 일실시예에서, 상기 트랜스미터(110)는 위성 방송 유닛일 수 있다. 대체 실시예에서, 전송 라인(115)은 무선이 아니라 케이블이다. 이 경우에, 트랜스미터(110)는 케이블 또는 유료 요금-TV 회사의 지상 기지 트랜스미터이다.

시스템(100)은 또한 디지털 방송 수신기 유닛(120)을 포함한다. 이러한 유닛(120)을 셋 탑 박스(STB)라고 부른다. 여기에서, 수신기 유닛(120)은 소스 장치(120)라고 부른다. 상기 소스 장치(120)는 아래에서 좀 더 설명된 다수의 EMI 통신 모드를 지원하기 위해, 본 발명에 따른 EMI 회로(150)를 포함한다. 회로(150)는 각각의 EMI 암호화 모드에 대해 다른 암호화 메커니즘을 사용한다. 상기 소스 유닛(120)은 지능 장치이고, 복사 방지 표준을 처리하기 위한 특수 회로를 포함한다. 예를 들어, 소스 유닛(120)은 채널(115)을 통해 디지털 프로그램을 수신하고 상기 디지털 프로그램은 복사 제어 정보(CCI 정보)를 사용하여 인코딩될 수 있다.

(120)과 연결된 싱크 장치(130)를 포함한다. 비록 BSR 장치로써 도시되었을지라도, 싱크 유닛(130)은 또한 도 8에 도시된 임의의 수신기 유닛일 수 있다. 많은 경우에 있어서, 상기 싱크 장치(130)는 상대적으로 간단한 장치이고, 복사 방지 표준을 완전하게 처리하기 위해 필요한 특수 회로의 전체 보완 소자를 포함하지는 않는데 이는 비용을 낮추기 위함이다. 예를 들어, 싱크 유닛(130)은 CCI로 코딩된 AV 정보를 디코딩 할 능력은 없다. 그러나, 상기 장치는 본 발명에 따른 EMI 회로(160)를 포함한다. EMI 회로(160)는 EMI 코드에 따라 암호화된 AV 정보 패킷을 해독할 수 있다. 싱크 유닛(130)은 직렬 라인(125)을 통해 상기 소스 유닛(120)으로부터 디지털 정보를 수신하기 위해 연결된다. 디지털 정보는 IEEE 1394 통신 표준을 사용하여 라인(125)을 통해 전달된다. 더욱이, 이러한 정보는 헤더 부분의 헤더 정보 및 데이터 부분의 AV 정보(예를 들어 데이터)를 포함하는 디지털 데이터 패킷에 전달된다.

아래에 좀 더 설명된 것처럼, 도 8의 EMI 회로(150 및 160)는 각각이 두 개의 암호 회로를 포함하도록 구현되는데 이는 라인(125)을 통해 전송된 정보가 최소한 두 개의 서로 다른 암호 메커니즘(A 및 B)하에서 인코딩 되도록 하기 위함이다. 일실시예에서, EMI 회로(160)는 또한 두 개의 암호 회로를 갖는데 이는 상기 회로가 (허용된다면) 모드(A) 암호화 또는 모드(B) 암호화에서 라인(125)을 통해 수신된 정보를 해독할 수 있도록 하기 위함이다. 본 발명은 BCI 코드를 사용하는 것보다는, 라인(125)의 데이터 패킷에 위치한 EMI 코드를 사용한다. 복사 방지 모드를 표시하는 것에 추가하여, 상기 EMI 코드는 또한 패킷의 데이터 부분에서 사용된 암호화 모드를 유리하게 결정한다. 그러므로, 싱크 유닛(130)의 상기 EMI 회로(160)는 라인(125)으로부터 수신된 전송을 해독하기 위해 적절한 해독 메커니즘을 선택하도록 EMI 모드를 선택한다. 본 발명의 EMI 코드가 싱크 장치(120)와 소스 장치(130) 사이에서(예를 들어, 중간 인터셉트 장치에 의해) 손상되었다면, 그 때 본 발명의 EMI 회로(160)는 잘못된 해독 모드를 선택할 것이다. 이 경우에, 상기 싱크 장치(130)에 의해 원래의 전송이 달성될 수는 없을 것이다.

디지털 인터페이스(125)를 통해 전송된 세 가지 종류의 AV 정보 패킷이 있다. 상기 정보 패킷은 자율 복사 정보, 일회 복사 정보, 및 금지된 복사 정보이다. 이러한 스트림들은 본 발명에 따른 복사 방지의 서로 다른 안전 레벨을 갖는다. 각각의 패킷에 복사 방지가 제공되는 방법을 각 패킷의 EMI 모드라고 부른다. 아래에 설명된 것처럼, 본 발명에 따라 상기 EMI 모드는 또한 상기 EMI 모드와 관련된 AV 정보에 적용된 암호화 모드를 표시한다.

본 발명에 따라 사용된 암호 또는 EMI 모드는 아래와 같이 설명된다. EMI 모드(A)는 패킷 데이터가 복사 금지임을 표시하기 위해 사용된다. 이러한 모드(A)하에서, AV 정보는 재생 장치(예를 들어, TV 또는 모니터)상에서만 단지 표현 될 수 있을 뿐이고 상기 AV 정보가 기록되는 것이 허용되지 않는다. EMI 모드(B)는 단일 생성 복사를 허용하기 위해 단 한 번만 AV 정보가 복사(예를 들어,기록)될 수 있음을 표시하기 위해 사용된다. 이 모드(B)는 또한 단일 복사 생성 허용 모드라고 불리운다. EMI 모드(O)는 AV 정보가 복사 방지를 갖지 않아서 복사의 제한이 없을 때 사용된다. 또한 상기 모드(O)를 무제한 모드라고 부른다. 설명의 간략화를 위해, 본 실시예에서는 모드(O)에 대한 암호화는 실행하지 않겠다. n개의 복사(n> 1)를 허용하는 복사 제어 상태에서 AV 정보의 경우에, 개별적인 n개-복사에 대응하는 모드를 한정함으로써 확장이 이루어질 수 있다.

상기 EMI 모드는 공지된 다수의 인코딩 기술을 사용하여 표현될 수 있고 최소한 2 비트를 가지는 레지스터를 사용하여 표현될 수 있다. 본 발명의 특정 일실시예에서, 2 비트의 레지스터가 사용된다. 아래의 표 1은 각 EMI 모드에 대한 예시적인 코딩 숫자를 도시한다. 표 1에서 선택된 코딩 숫자는 단지 예시적인 것일 뿐이고 세 개의, 고유 숫자로 구성된 임의의 세트가 사용될 수 있음이 이해된다.

[표1]

*EMI*모드	2비트숫자	설명
모드(*A*)	11	복사금지
모드(*B*)	10	일회복사
모드(*O*)	00	비암호화이고 무제한
예비	01	

디지털 인터페이스(125)를 통해 수신된 AV 정보는 다수의 프로그램을 포함할 수 있다는 것이 인지된다. 각 프로그램은 각자의 복사 안전 레벨을 가질 수 있다. 이 경우에, 복사 금지 스트림{코드(11)}은 최소한 일회의 복사조차 금지된 프로그램을 포함하는 스트림이다. 일회 복사 스트림{코드(10)}은 복사가 금지되지 않은 프로그램을 가지고 최소한 한 번의 일회 복사 프로그램을 포함하는 스트림이다. BSR 싱크 장치(130)(도 3)의 특정 예에서, 장치(130)는 EMI 모드(B){또는 EMI 모드(O)}에서 수신된 AV 정보만을 기록할 수 있고 EMI 모드(A)에서 수신된 AV 정보를 단순히 통과(또는 거절)시킬 수 있다.

도 4는 소스 유닛(120)으로부터 싱크 유닛(130)으로 전송(도 3)되는, 본 발명에 따른 전형적 정보 패킷(200)을 구성하는 필드를 도시한다. 도 4의 정보 패킷(200)은 IEEE 1394 헤더 섹션(230)을 포함하는데, 이것은 이 실시예에서 상기 데이터 패킷이 IEEE 통신 표준을 따르기 때문이다. 이러한 헤더 섹션(230)은 데이터_길이 필드, 태그 필드, 채널 필드, t코드 필드 및 sy 필드를 포함한다. 태

데이터 필드가 CIP 헤더(240)에서 시작한다는 것을 표시한다. 상기 t코드 필드는 미리 결정된 두 개의 값 중 하나일 수 있다. 데이터 스트림은 하나의 1394 등시성 채널상의 정보 스트림을 의미함이 인식된다.

정보 패킷(200)은 또한 CIP 헤더 섹션(240)을 포함한다. 본 발명에 따라, CIP 헤더 섹션(240)은, 하나의 구현에서 2 비트의 폭이고 표 1에서 정의된 것과 같은 EMI 모드 값을 포함하는 EMI 필드(210)를 포함한다. 상기 EMI 모드 값은 섹션(250)의 데이터 필드(220)의 데이터와 관련된 특정 안전 통신 모드에 대응한다. 아래에 좀더 설명된 것처럼, 상기 EMI 필드(210)에 표시된 EMI 모드는 :(1)선택된 특정 안전 통신 모드{예를 들어, 모드(A), 모드(B) 또는 모드(O)} 및 또한 (2)패킷(200)에 대해 사용된 특정 유형의 암호화 기술을 표시한다. 본 발명이 {만일 EMI 모드(A) 또는 EMI 모드(B)에 있다면}패킷(200)의 데이터 부분(220)을 암호화시키는 반면, IEEE 1394 인터페이스(125)(도 3)를 통해 전송될 때 헤더 섹션(230 및 240)은 암호화되지 않고 남아 있다는 것이 인식된다.

필드(210)의 EMI 모드는 1394 등시성 스트림상에 있는 데이터 스트림의 복사 제어 상태를 표시한다. 본 발명에 따른 데이터 스트림이 몇몇 비디오 및/또는 오디오 프로그램을 구성할 수 있고 각 프로그램은 프로그램과 관련된 서로 다른 복사 제어 정보를 가질 수 있다는 것을 이해하는 것이 중요하다. 예를 들어, 소스 유닛으로부터의 MPEG 이송 스트림 출력은 몇몇 프로그램을 포함할 수 있고 각 프로그램에 대해 서로 다른 복사 방지 레벨을 가질 수 있다. 소스 장치는 스트림내에서 가장 제한적인 프로그램에 대해 EMI 값을 할당한다. 비트 스트림 기록기는 상기 EMI 값에 기초한 전체 스트림을 기록할 수도 있고 기록하지 않을 수도 있다. 상기 스트림에서 각 프로그램을 개별적으로 처리할 수 있고, 또한 각 프로그램과 관련된 복사 제어 정보를 해석할 수 있는, 또다른 유형의 기록 장치를 포맷 인식 기록 장치라고 부른다. 포맷 인식 기록 장치는 동작을 결정하기 위해 각 프로그램과 관련된 제어 정보를 참조한다.

본 발명의 EMI 회로

도 5a는 소스 장치(120) 및 싱크 장치(130)를 구비하는, 본 발명의 시스템(400)을 도시한다. 도 5a는 전형적인 소스 유닛(120)의 EMI 회로(150)를 좀 더 자세하게 도시한다. 소스 유닛(120)은 상기 EMI 회로(150)에 추가하여 많은 공지된 회로들(명확히 도시되어 있지는 않지만)을 포함하는 방송 수신기로 또한 지칭되는 셋-탑-박스(STB) 일수 있다. 수신기 회로(410)는 데이터 패킷의 형태로 AV 정보를 수신하고 CCI 표준하에서 요구되는 임의의 해독을 수행한다. 그 결과치는 통신 인터페이스(430)를 통해 전달되고, 인터페이스(413)를 이용하여 또한 디멀티플렉서(de-mux)(414)로 전달된다. 회로(412)는 EMI 모드 선택 회로이고, 만일 복사 방지가 필요하다면 회복된 CCI 복사 방지 정보에 따라 상기 회로는 EMI 모드(A) 또는 EMI 모드(B)를 선택할 것이다. 만일 복사 방지가 필요치 않다면, 그 때 인터페이스(413)가 인터페이스(125)로 직접 통과되고, EMI 모드(O)(코드"0")가 상기 데이터 패킷의 EMI 필드(210)로 삽입된다.

복사 방지가 필요하다고 가정하면, 선택 회로(412)는 라인(426)을 통한 신호를 통해 디멀티플렉서(414)를 제어한다. 만일 EMI 모드(A)가 선택된다면, 그 때 (413)으로부터의 데이터 패킷은 암호 키(416) 및 암호화 유닛A(418)내의 제 1 암호화 기술에 따라 상기 데이터 패킷의 데이터 부분{예를 들어, 필드(220)}을 암호화하는 암호화 유닛A(418)로 전달된다. 유닛(418)은 또한 데이터 패킷의 EMI 모드 필드(210)내에 코드("11"){EMI 모드(A)}를 위치시킨다. 그 때 결과치는 또한 라인(426)에 의해 제어되는 멀티플렉서(mux)(422)로 전달된다. 멀티플렉서(422)는 암호화 유닛A(418)으로부터의 출력을 선택적 출력 드라이버(424)를 사용하여 인터페이스(125)로 전달한다. 만일 EMI 모드(B)가 선택된다면, 그 때 (413)으로부터의 데이터 패킷은 상기 키(416) 및 암호화 유닛 B(420)내의 제 2 암호화 기술에 따라 상기 데이터 패킷의 데이터 부분{예를 들어, 필드(220)}을 암호화하는 암호화 유닛 B(420)으로 전달된다. 유닛(420)은 또한 데이터 패킷의 EMI 모드 필드(210)내에 코드("10"){EMI 모드(B)}를 위치시킨다. 그 때 결과치는 또한 라인(426)에 의해 제어되는 멀티플렉서(mux)(422)로 전달된다. 멀티플렉서(422)는 암호화 유닛 B(420)로부터의 출력을 선택적 출력 드라이버(424)를 사용하여 인터페이스(125)로 전달한다. 이러한 실시예에서, 두 개의 서로 다른 암호화 유닛이 또한 사용되고, 상기 암호화는 두 개의 암호화 메커니즘을 제공하기 위해 공통 키 값(416)에 기초한다. 아래에서 좀 더 설명되었듯이, 상기 키(416)는 소스-싱크 확인 과정 동안에 확립될 수 있다.

도 5a의 싱크 장치(130)는 EMI 회로(160)에 추가하여 많은 공지된 회로들(명확하게 도시되어 있지는 않지만)을 포함한다. 도 5a의 싱크 장치(130)내의 EMI 회로(160)는, 암호 키(452)가 키(416)와 부합한다고 가정하면 암호화 유닛A(418)에 의해 수행된 암호화를 해독할 수 있는 해독 유닛 A(448)을 포함하고, 키(452)가 올바르다고 가정하면 암호화 유닛 B(420)에 의해 수행된 암호화를 해독할 수 있는 해독 유닛 B(450)를 포함한다. 인터페이스(125)의 데이터 패킷은 디멀티플렉서 회로(442) 및 또한 EMI 모드 추출기 회로(440)에 의해 수신된다. 회로(440)는 상기 수신된 데이터 패킷으로부터 헤더 정보를 추출하고 상기 헤더로부터 EMI 필드(210)를 추출한다. 추출된 EMI 모드에 따라, 회로(440)는 라인(446)을 통해 신호를 제어한다. 만일 EMI 모드(O)가 추출된다면, 그 때 라인(125)을 통한 데이터 패킷은 직접 비트 스트림 기록 매체(456)에 연결되거나 금지 표시 없이 라인(470)을 통해 직접 출력됨이 허용된다.

만일 회로(440)가 EMI 모드(A)를 추출한다면, 그 때 인터페이스(125)로부터의 데이터 패킷은 상기 데이터 패킷의 데이터 부분을 {키(452)를 사용하여} 해독하는 해독 유닛 A(448)로 디멀티플렉서(442)를 통해 전달되고, 그 결과치를 선택 라인(446)에 의해 또한 제어되는 멀티플렉서(454)로 전달한다. 멀티플렉서(454)는 해독 유닛 A(448)의 출력으로부터의 데이터 패킷을 출력 라인(470)으로만 전달한다. 싱크 장치(130)가 BSR 장치일 때, EMI 모드(A) 데이터 패킷을 기록하는 것이 허용되지 않으므로 이 경우 상기 BSR 매체(456)에 기록하는 것은 금지된다. 만일 회로(440)가 EMI 모드(B)를 추출하면, 그 때 인터페이스(125)로부터의 데이터 패

모드(A)로 변화시키며, 상기 EMI 필드(210)에 코드("11")(모드 A)를 기록하고 그 결과치를 선택 라인(446)에 의해 또한 제어되는 멀티플렉서(454)로 전달한다. 현 EMI 모드(A)에서, 멀티플렉서(454)는 해독 유닛 B(450)의 출력으로부터의 데이터 패킷을 출력 라인(470)으로 전달하고, 상기 BSR 매체(456)가 상기 데이터 패킷을 기록하도록 허용한다. 상기 싱크 장치(130)가 BSR 장치일 때, EMI 모드(B) 데이터 패킷을 단지 일 회 기록하는 것이 허용되므로 이러한 데이터 패킷은 상기 BSR 매체(456)에서 기록하기 전에 EMI 모드 (A) 패킷으로 변화된다. 이러한 실시예에서, 두 개의 서로 다른 해독 유닛이 사용되고, 상기 해독은 단일 암호 키(452)에 기초한다.

상기 싱크 장치(130)가 비트 스트림 기록(BSR) 장치일 때, EMI 모드(A)에서 암호화된 데이터를 기록하는 것은 허용되지 않는다. 그러므로, EMI 모드(A)에 대한 해독 유닛 A는 BSR에서 구현되지 않는다. 도 6a는 해독유닛 A가 없는 비트 스트림 기록 싱크 장치(130)에 대한 EMI 회로의 대체 실시예의 블록도(665)이다. 이러한 실시예에서, 만일 상기 EMI 추출기(440)가 입력(125)에서 모드(A)를 검출하면, 상기 추출기는 해독 유닛 B를 정지시키고 상기 BSR 기록 유닛(456)을 정지시킨다.

도 5a의 회로(400)는 중간 장치가 다음과 같은 방법으로 복사 방지를 저하시키는 것을 막는다. 만일 EMI 모드(A) 데이터 패킷이 라인(125)상에서 EMI 모드(B) 데이터 패킷으로 바뀐다면, 상기 싱크 장치(130)는 데이터를 회복하려고 할 때 잘못된 해독 유닛을 사용할 것이다. 그 결과치는 BSR 매체(456)에 의해 기록된 의미 없는 정보가 된다. 만일 인터페이스(125)로부터의 EMI 모드(A) 또는 EMI 모드(B) 데이터 패킷이 EMI 모드(O) 데이터 패킷으로 바뀐다면, 그 때 싱크 장치(130)는 어떠한 해독도 수행하지 않을 것이고 그 결과치는 나타낼 수 없게 된다.

도 5b는 소스 장치(120')와 싱크 장치(130')를 구비하는, 본 발명의 시스템(500)을 도시한다. 도 5b는 본 발명의 대체 실시예의, 전형적 싱크 유닛(130')의 EMI 회로(160') 및 전형적 소스 유닛(120')의 EMI 회로(150')를 도시한다. 이러한 실시예에서, 공통의 암호 유닛 및 공통의 해독 유닛이 사용되지만, 선택된 EMI 모드에 따라 상기 유닛들은 서로 다른 암호 키(키 A, 키 B)를 수신한다; 이는 두 개의 암호-해독 메커니즘을 제공한다.

도 5b의 소스 유닛(120')은 상기 EMI 회로(150')에 추가하여 많은 공지된 회로들(명확히 도시되어 있지는 않지만)을 포함하는 방송 수신기로 또한 지칭되는 셋-탑-박스(STB) 유닛일 수 있다. 수신기 회로(510)는 데이터 패킷의 형태로 AV 정보를 수신하고 CCI 표준하에서 요구되는 임의의 해독을 수행한다. 그 결과치는 {EMI 모드가 선택된 회로(514)에 연결된}통신 인터페이스(512)를 통해 전달되고, 또한 인터페이스(513)로 향한다. 회로(514)는 EMI 모드 선택 회로이고, 만일 복사 방지가 필요하다면 회복된 CCI 복사 방지 정보에 따라 EMI 모드(A) 또는 EMI 모드(B)를 선택할 것이다. 만일 복사 방지가 필요치 않다면, 그 때 인터페이스(513)가 인터페이스(125)로 직접 통과되고 EMI 모드(O)(코드"0")가 상기 데이터 패킷의 EMI 필드(210)로 삽입된다.

복사 방지가 필요하다고 가정하면, 선택 회로(514)는 멀티플렉서(mux)(516)의 선택 라인을 제어한다. 공통 키(524)는, 출력에 제 1 암호 키(키 A)를 생성시키고 제 1 해시(hash) 함수를 가지는 해시 회로 A(520)에 전달된다. 키(524)는 또한, 출력에 제 2 암호 키(키 B)를 생성시키고 제 2의 다른 해시(hash) 함수를 가지는 해시 회로 B(522)에 전달된다. 만일 EMI 모드(A)가 선택된다면, 그 때 멀티플렉서(516)는 키(A) 및 암호화 유닛(518)내의 공통 암호화 기술에 따라 상기 데이터 패킷의 데이터 부분{예를 들어, 필드(220)}을 암호화하는 공통 암호화 유닛(518)으로 전달하기 위해 키(A)를 선택한다. 유닛(518)은 또한 데이터 패킷의 EMI 모드 필드(210)내의 코드("11"){EMI 모드(A)}를 위치시킨다. 그 때 결과치는 인터페이스(125)로 데이터 패킷을 출력하는 선택적 드라이버 회로(526)로 인터페이스(530)을 통해 전달된다.

만일 EMI 모드(B)가 선택된다면, 그 때 도 5b의 멀티플렉서(516)는 키(B) 및 암호화 유닛(518)내의 공통 암호화 기술에 따라 상기 데이터 패킷의 데이터 부분{예를 들어, 필드(220)}을 암호화하는 공통 암호화 유닛(518)으로 전달하기 위해 키(B)를 선택한다. 유닛(518)은 또한 데이터 패킷의 EMI 모드 필드(210)내에 코드("10"){EMI 모드(B)}를 위치시킨다. 그 때 결과치는 인터페이스(125)로 데이터 패킷을 출력하는 선택적 드라이버 회로(526)로 인터페이스(530)를 통해 전달된다. 이러한 실시예에서, 두 개의 서로 다른 키(A 및 B)가 단일 공통 암호화 유닛(518)에서 사용된 암호화 과정을 변화시키기 위해 사용된다. 아래에 설명된 것처럼, 키(524)는 소스-싱크 확인 과정 동안에 확립될 수 있다. 코버트(covert) 채널 키(Kc)를 공유한 후에, 상기 소스 장치(120') 및 상기 싱크 장치(130')는 저작물 키(A 및 B)를 공유한다. 먼저, 소스 장치(120')는 무작위 수(Na)를 싱크 장치(130')에 보낸다. 상기 소스 장치 및 싱크 장치는 다음 식에 의해 저작물 키{키(A) 및 키(B)}를 계산하기 위해 내부의 EMI 회로를 이용한다:

Key A=HKc(Na || Ca)

Key B=HKc(Na || Cb)

여기서 키(Kc)를 사용한 키 해시 함수(Hkc)에서, Ca 및 Cb는 상수이자 허용 코드이다.

회로(150')는 단지 단일 암호화 유닛(518)만을 필요로 하기 때문에 유리하다. 비록 두 개의 해시 함수 회로(520, 522)가 필요하다 할지라도, 이러한 추가 회로는 일반적으로, 제 2 암호화 유닛을 제거함으로써 제거되는 회로보다는 더 적다. 만일 해시 함수가 소프트웨어로 구현된다면 이는 특히 사실이다. 해시 함수는 주어진 키에 대해 오직 한 번만 결정됨을 필요로 하기 때문에 소프트웨어로 쉽게 구현될 수 있다.

도 5b의 싱크 장치(130')는 EMI 회로(160')에 추가하여 다수의 공지된 회로들(명확히 도시되어 있진 않지만)을 포함한다. 정확한 공통 키가 제공된다고 가정하면, 상기 싱크 장치(130')내의 EMI 회로(160')는 공통 암호화 유닛(518)에 의해-수행된 암호화를 해독할 수 있는 단일 공통 해독 유닛(544)을 포함한다. 인터페이스(125)의 데이터 패킷은 EMI 모드 추출기 회로(540)에 의해 수신된다. 회로(440)에서처럼, 회로(540)도 상기 수신된 데이터 패킷으로부터 헤더 정보를 추출하고 상기 헤더로부터 EMI 필드(210)를 추출한다. 추출된 EMI 모드에 따라, 회로(540)는 멀티플렉서(542)의 선택 라인을 제어한다. 만일 EMI 모드(O)가 회로(540)에 의해 추출된다면, 그 때 라인(125)을 통한 데이터 패킷은 비트 스트림 기록 매체(550)에 직접 연결되거나 라인(570)을 통해 직접 출력되도록 허용된다.

복사 방지 모드가 추출되었다고 가정하면, EMI 추출 회로(540)는 멀티플렉서(mux)(542)의 선택 라인을 제어한다. 키(554)는 출력에 제 1 암호 키(키 A)를 생성시키고 제 1 해시 함수를 가지는 해시 회로A(546)에 전달된다. 키(554)는 또한 출력에 제 2 암호 키(키 B)를 생성시키고 제 2의 다른 해시 함수를 가지는 해시 회로B(548)에 전달된다. 만일 EMI 모드(A)가 데이터 패킷으로부터 추출된다면, 그 때 멀티플렉서(542)는 키 A 및 해독 유닛(544)내의 공통 해독 기술에 따라 상기 데이터 패킷의 데이터 부분{예를 들어, 필드(210)}을 해독하는 공통 해독 유닛(544)으로 전달하기 위해 키(A)를 선택한다. 유닛(544)은 또한 상기 데이터 패킷의 EMI 모드 필드(210)내에 코드("11"){EMI 모드 (A)}를 위치시킨다. 그 결과치는 단지 출력 라인(570)으로만 전달된다. 상기 싱크 장치(130')가 BSR 장치일 때, EMI 모드(A) 데이터 패킷을 기록하는 것이 허용되지 않으므로 이 경우, 상기 BSR 매체(550)에 기록하는 것은 금지된다.

만일 EMI 모드(B)가 회로(540)에 의해 추출된다면, 그 때 도 5b의 멀티플렉서(542)는 키(B) 및 해독 유닛(544)내의 공통 해독 기술에 따라 상기 데이터 패킷의 데이터 부분{예를 들어, 필드(220)}을 해독하는, 공통 해독 유닛(544)으로 전달하기 위해 키(B)를 선택한다. 유닛(544)은 또한 데이터 패킷의 EMI 모드 필드(210)내에 코드("11"){EMI 모드(A)}를 위치시킨다. 현 EMI 모드(A)에서, 그 때 결과치는 인터페이스(552)를 통해 BSR 기록 매체(550)로 전달되고 선택적으로는 출력 인터페이스(570)로 전달된다. 싱크 장치(130')가 BSR 장치일 때, EMI 모드(B) 데이터 패킷을 단지 한 번만 기록하는 것이 허용되므로 이러한 데이터 패킷은 상기 BSR 매체(550)에 기록하기 전에 EMI 모드(A)로 변화된다. 이러한 실시예에서, 두 개의 서로 다른 키(A 및 B)는 단일 공통 해독 유닛(544)에서 사용된 해독 과정을 변화시키기 위해 이용된다. 아래에서 좀 더 논의되었듯이, {키(524)에서처럼}키(554)는 소스-싱크 확인 과정 동안에 확립될 수 있다. 회로(160')는 단지 단일 해독 유닛(544)만을 필요로 하기 때문에 유리하다. 비록 두 개의 해시 함수 회로(546, 548)를 필요로 하지만, 이러한 추가 회로는 일반적으로, 상기 제 2 해독 유닛을 제거함으로써 제거된 회로보다는 더 적다. 해시 함수(546, 548)는 주어진 키에 대해 단지 한 번만 결정됨이 필요하기 때문에 소프트웨어로 쉽게 구현된다.

상기 싱크 장치(130')가 비트 스트림 기록(BSR) 장치일 때, EMI 모드(A)에서 암호화된 데이터를 기록하는 것이 허용되지 않는다. 그러므로, EMI 모드(A)에 대한 해시 A 회로는 BSR에서 구현되지 않는다. 도 6b는 상기 해시 A 회로가 없는 비트 스트림 기록 싱크 장치(130')에 대한 EMI 회로의 대체 실시예의 블록도(670)를 도시한다. 이러한 실시예에서, 만일 EMI 추출기(540)가 입력(125)에서 모드 (A)를 검출한다면, 상기 추출기는 공통 해독 유닛(544)을 정지시키고 상기 BSR 기록 유닛(550)을 정지시킨다.

도 5a의 회로(500)는 중간 장치가 다음의 방법으로 복사 방지를 저하시키는 것을 막는다. 만일 EMI 모드(A) 데이터 패킷이 라인(125)상에서 EMI 모드(B) 데이터 패킷으로 바뀐다면, 싱크 장치(130)는 상기 데이터를 회복시키려고 할 때 (키 A 및 키 B 사이의) 잘못된 해독 키를 사용할 것이다. 그 결과치는 BSR 매체(550)에 의해 기록된 의미 없는 정보이다. 만일 인터페이스(125)로부터의 EMI 모드(A) 또는 EMI 모드(B) 데이터 패킷이 EMI 모드(O) 데이터 패킷으로 바뀐다면, 그 때 싱크 장치(130')는 어떠한 해독도 수행하지 않을 것이고 그 결과치는 나타낼 수 없다.

도 7은 도 5a의 시스템(400)에 관해 본 발명에 의해 수행된 단계의 흐름도(700)이다. 단계(710)에서, 싱크 장치와 소스 장치가 서로를 인식했는지를 위해 확인 과정이 수행된다. 이러한 과정은 미리 결정된 다양한 허가 및 서비스 키를 사용하여 수행될 수 있다. 임의의 다수의 공지된 확인 과정 및 안전 키 교체 과정은 본 발명에 따라 단계(710)에서 사용될 수 있다. 결과적으로, 만일 확인 과정이 성공적으로 되면 특수 코드가 교체되고, 단계(720)가 입력된다. 단계(715)에서 만일 확인이 실패하면, 어떠한 AV 정보 교체 없이 과정(700)이 복귀한다.

도 7의 단계(720)에서, 소스 장치(120)는 키를 해독하는 싱크 장치(130)로 암호화된 키를 보내기 위해 특수 코드를 사용한다. 이 시점에서, 키(416 및 452)는 소스 장치와 싱크 장치 사이에서 확립되고 이러한 키들은 동일한 값을 갖는다. 단계(730)에서, 소스 장치(120)는 제 1 복사 방지 모드를 갖는 데이터 패킷을 (예를 들어 CCI모드를 사용하여)수신하고, 이러한 CCI 모드를 EMI 모드(예를 들어, 복사 금지, 일회 복사, 무제한 복사)로 변환시킨다. 단계(740)에서, 회로(150)는 적절한 EMI 모드를 상기 수신된 데이터 패킷의 헤더로 위치시키고, 상기 EMI 모드에 따라 가능한 두 개의 암호화 메커니즘 중의 하나를 사용하여 상기 데이터 패킷의 데이터 부분을 암호화한다. 그 때 이러한 데이터 패킷은 인터페이스(125)를 통해 전달된다.

도 7의 단계(740)에서, 싱크 장치는 EMI 모드를 추출하고 추출된 EMI모드에 따라 데이터 패킷을 해독하기 위해 회로(160)를 사용한다. 두 개의 가능한 해독 메커니즘 중의 하나가 EMI 모드에 기초하여 사용된다. 만일 EMI 모드(B)가 수신된다면, 이러한 정보는 EMI 모드(A)(완전한 방지)에 기록된다. 만일 EMI 모드(A)가 수신되었다면, 그 때는 어떠한 기록도 허용되지 않는다. 단계(760)에서 만일 좀 더 많은 데이터 패킷이 필요하다면, 다음 데이터 패킷을 처리하기 위해 과정(700)이 단계(740)로 복귀한다. 그렇지 않

도 5b의 대체 실시예의 동작 과정은 서로 다른 키가 도 5b의 다른 암호 및 해독 메커니즘을 제공하기 위해 사용된다는 것을 제외하고는 위의 과정과 비슷하다.

본 발명에 따른 장치의 분류

도 8은 본 발명에 따라 사용될 수 있는 장치의 다수의 다른 분류를 도시한다. 또한 각각의 장치에 의해 송수신될 수 있는 (EMI 모드에 의해 분류된)AV 정보 패킷의 유형이 도 8에 도시된다. 점선의 신호 라인은 EMI 모드(B)의 AV 정보 패킷을 나타내고 실선의 신호 라인은 EMI 모드(A)의 AV 정보 패킷을 나타낸다. 제 1 장치 분류는 장치 분류(A)이다. 이러한 장치는 패킷 정보에 EMI 코드를 추가할 수 있는 전송 장치를 포함하고 또한 CCI 데이터를 수신할 수 있는 수신 장치를 포함한다. 일예는 IEEE 1394 버스를 통해 데이터를 전송하고 (예를 들어, CCI 포맷으로)위성 방송을 수신할 수 있는 셋-박스(STB)(120)이다. 도 8에 도시된 것처럼, 상기 STB 장치(120)는 EMI 모드(A) 또는 EMI 모드(B)에서 암호화된 AV 전송 패킷을 생성할 수 있다. 상기 STD 장치(120)는 또한 제한 없는 AV 정보를 생성할 수 있다. 장치(120)는 출력(626)에 의해 보여지는 것처럼 EMI 모드(B)로 AV 정보를 제공하고 출력(628)에서 보여지는 것처럼 EMI 모드(A)로 AV 정보를 제공한다.

제 2 장치 분류는 장치 분류(B)이다. 이러한 장치는 AV 정보 패킷에서 나타내는 EMI 정보에 응답할 수 있는 수신 또는 싱크 장치를 포함한다. 분류(B)내의 예시적 장치는 포맷 인식 기록 장치(630)이다. 이러한 장치(630)는 임의의 EMI 모드에서 수신된 AV 정보 패킷을 적절히 해독할 수 있고, IEEE 1394 표준 포맷을 사용하여 AV 정보를 기록할 수 있고, 상기 AV 정보에 추가된 EMI 정보를 기록할 수 있으며, 재생된 데이터를 상기 IEEE 1394 표준 포맷을 사용하여 전송할 수 있다. 만일 상기 수신된 AV 정보가 EMI 모드(B)에서 비롯되었다면, 기록될 때 그 이상의 복사를 막기 위해 상기 모드(B)는 EMI 모드(A)로 변화된다. 장치(630)는 EMI 모드(A)(634) 및 EMI 모드(B)(632)에서 암호화된 AV 정보 패킷을 수신할 수 있지만 EMI 모드(A)(636)에서 암호화된 AV 정보만을 제공할 수 있다.

제 3 장치 분류는 장치 분류(C)이다. 이러한 장치는 (예를 들어, CCI 모드에서)특정 복사 방지 정보를 완전히 처리할 수는 없는 수신 장치를 포함하는데, 그 이유는 이러한 장치는 이러한 복사 방지 정보를 완전히 처리하기 위해 필요한 특수 회로가 결여되어 있기 때문이다. 분류(C)의 일례는 도 8의 비트 스트림 기록기(BSR) 장치(130)이다. 상기 장치는 입력(610)을 통해 EMI 모드(B)에서 암호화된 AV 정보만을 수신하는 것이 가능하고, 출력(615)을 통해 EMI 모드(A)에서 해독된 AV 정보만을 제공할 수 있다. 만일 EMI 모드(B)가 수신되면, 상기 BSR 장치(130)는 추출된 EMI 코드를 사용하여 모드(B) 암호화를 해독할 수 있고, 이러한 정보를 저장할 수 있다. 상기 BSR 장치(130)는 또한 AV 정보를 재생할 수 있고 이 정보를 IEEE 1394 표준하에서 EMI 모드(A)로 전송할 수 있다.

제 4 장치 분류는 장치 분류(D)이다. 이러한 장치는 정보 패킷에 추가된 EMI 정보를 처리할 수 있는 수신 장치를 포함한다. 분류(D) 장치의 예는 디지털 텔레비전(620)이다. IEEE 1394 표준하에서, 상기 디지털 TV 수상기(620)는 입력(622)을 통해 EMI 모드(B)에서 암호화된 AV 정보 및 입력(624)을 통해 EMI 모드(A)에서 암호화된 AV 정보를 수신할 수 있다. 상기 디지털 TV(620)는 EMI 모드(A) 또는 EMI 모드(B)로부터의 AV 정보를 해독할 수 있고 상기 AV 정보를 나타낼 수 있다.

암호화 및 해독 모드는 개체(entity)가 달성하기를 원하는 기능에 따라 상기 개체에 의해 허가될 수 있다. 만일 상기 개체가 디스플레이 장치를 제조한다면, EMI 모드(A) 및 EMI 모드(B)의 해독에 대한 허가가 필요하다. 만일 상기 개체가 BSR 유닛(130)을 제조한다면, EMI 모드(A)에 대한 암호화 및 EMI 모드(B)에 대한 해독이 필요하다. 본 발명의 일실시예에 관해 아래에 설명되었듯이, EMI 모드(A 및 B)는 허가 키 및 서비스 키와 결합될 수 있다.

본 발명의 일실시예에 따른 예시적인 서비스 분류

본 발명의 일실시예에서, 특정 통신 서비스가 지원된다. 이러한 실시예에서, 특정 비밀 암호(예를 들어, 키 코드)는 사용된 서비스 유형에 따라 그리고 장치가 소스 장치인지 싱크 장치인지에 따라 정의된다. 전송 장치 및 수신 장치의 위의 분류에 따라, 다음은 데이터 전송에 대한 서비스 분류를 표시한다. 서비스(1)내의 전송은 분류(A, B, 또는 C)의 수신 장치를 갖는 분류(A, B, 또는 C)의 전송 장치를 포함한다. 서비스(2)내의 전송은 분류(D)의 수신 장치를 갖는 분류(A, B, 또는 C)의 전송 장치를 포함한다. 서비스(3)내의 전송은 분류(A, B, 또 C)의 수신 장치를 갖는 분류(D)의 전송 장치를 포함한다.

일반적으로, 서비스(1)에서, CCI 복사 방지 포맷을 인식하는 소스 유닛은 또한 이러한 CCI 포맷을 인식하는 싱크 유닛으로 AV 정보를 전송한다(예를 들어, STD --> 디스플레이, 또는, STB --> 포맷 인식 기록기). 소스 및 싱크 모두 복사 방지 지능 장치이다. 서비스(2)에서, CCI 포맷을 인식하는 소스 유닛은 또한 이러한 CCI 포맷을 인식하지는 않지만 본 발명에 따라 EMI 코드를 인식하기 위해 구현되는 싱크 유닛으로 AV 정보를 전송한다(예를 들어,STB--> BSR 유닛). 이러한 싱크 유닛은 상기 소스 유닛과 동일한 레벨의 복사 방지 지능을 갖지는 않는다. 서비스(3)에서, CCI 포맷을 인식하지 못하는 소스 유닛은 CCI 포맷을 인식하는 싱크 유닛으로 AV 정보를 전송한다(예를 들어, DVHS--> 디스플레이).

본 발명의 일실시예에서, EMI 모드(A)와 EMI 모드(B) 및 서비스(1, 2, 및 3)을 이용하기 위한 비밀 암호 코드(예를 들어, 키 코드)는 위에서 열거된 각각의 분류 장치에 제공된다(예를 들어. 허가된다). 키 코드 또는 "비밀 암호"는 위에서 설명된 것처럼, 확인 동안

된 키는 소스 및 싱크 장치 사이로 안전하게 전송될 수 있다.

서비스(1, 2, 및 3)에서, 서로 다른 키 코드가 전송 장치 및 수신 장치를 위해 필요하다. 예를 들어, 서비스(1)의 전송 장치에 대한 키 코드는 수신 장치에 대한 키 코드와는 다르다. 여기에는 상기 키 코드가 각각의 장치에 제공되는 방법이 설명된다. 도 9의 테이블에 따라, 본 발명의 실시예의 이러한 실시예에서 사용된 8개의 키 코드가 있다. 상기 장치의 분류는 MPEG 또는 DV 와 같은 유형의 데이터에 따라 더 자세히 분류될 수 있다. 하나의 서비스 키 및 허가 키를 포함하는 한 쌍은 서비스(1, 2, 및 3)에 각각 할당된다. 소스 유닛은 서비스 키를 갖고 싱크 유닛은 지원되는 서비스에 따라서 대응하는 허가 키를 갖는다. 그러므로, 서비스(1, 2, 및 3)는 서비스 키 또는 허가 키에 의해 구별된다.

예를 들어, STB 유닛(120)은 서비스(1, 2)를 제공할 수 있으므로, 상기 STB 유닛(120)은 서비스 키(1 및 2)를 가진다. DVHS(130)는 서비스(2)를 수신할 수 있고 서비스(3)를 제공할 수 있으므로 DVHS(130)는 허가 키(2) 및 서비스 키(3)를 갖는다. 각 서비스는 자신의 서비스 그룹 내에서 서브 서비스로 세분될 수 있다. 암호화 모드, 서비스 모드, 및 허가 키의 한 세트는 장치가 가져야만 하는 기능에 따라 유닛에 제공된다. 예를 들어, 디스플레이 장치(620)는 암호화 EMI 모드(A) 및 EMI 모드(B) 그리고 서비스(1, 3)를 위한 허가 키를 가질 수 있다. STB 유닛(120)은 EMI 모드(A) 및 EMI 모드(B)에 대한 암호화 및 서비스(1, 2)에 대한 서비스 키를 가질 수 있다. DVHS(BSR) 유닛(130)은 EMI 모드(B)에 대한 해독, EMI 모드(A)에 대한 암호화 및 서비스(2)에 대한 허가 키 및 서비스(3)에 대한 서비스 키를 가질 수 있다.

도 9에 따라, 분류(A)의 장치는 EMI 모드(A) 및 EMI 모드(B)에 대한 키 코드 및 서비스(1 및 2)의 전송 장치를 위한 키 코드를 갖는 것이 필요하고, 또 키 코드: 시크리트 1T;시크리트 1T;시크리트 2T;시크리트 2T;시크리트 A 및 시크리트 B가 제공된다. 유사하게, 분류(B) 장치는 서비스(1 및 3)의 수신 장치에 대한 키 코드 및 서비스(1)의 전송 장치에 대한 키 코드 및 모드(A 및 B)에 대한 키 코드를 갖는 것이 필요하고 또 키 코드들: 시크리트 1R;시크리트 1R;시크리트 3R;시크리트 3R;시크리트 A:시크리트 B가 제공된다. 분류(C) 장치는 서비스(1 및 3)의 수신 장치에 대한 키 코드 및 모드(A 및 B)에 대한 키 코드를 갖는 것이 필요하고 또 키 코드들: 시크리트 1R;시크리트 1R; 시크리트 3R;시크리트 3R;시크리트 A:시크리트 B가 제공된다. 분류(D) 장치는 서비스(2)의 수신 장치에 대한 키 코드 및 서비스(3)의 전송 장치에 대한 키 코드를 갖는 것이 필요하고 또 키 코드들: 시크리트 2R;시크리트 3T;시크리트 A:시크리트 B가 제공된다. 일반적으로, 전송만을 위한 모드(A)의 사용 및 수신만을 위한 모드(B)의 사용이 요구된다.

서비스 키를 이용한 본 발명의 동작

다음의 과정은 데이터 패킷이 분류(A)의 소스 장치로부터, 수신 장치로써 동작하는 분류(B)의 싱크 장치로 전송되는 방법을 설명한다. 상기 데이터 패킷은 소스 장치로부터 싱크 장치로 전송되고 상기 싱크 장치에 의해 기록된다.

전송 측에서의 소스 장치는 상기 데이터 패킷을 암호화하기 위한 데이터 키로써 K시드(Kseed)를 발생시킨다. 상기 소스 장치는 서비스(1)의 전송 장치 및 수신 장치에 대한 비밀 암호(시크리트 1T 및 시크리트 1R)를 사용하여 수신측에서의 싱크 장치로 상기 데이터 키(K시드)를 안전하게 전송한다. 다음에, 상기 소스 장치는 K시드, 시크리트 A, 및 시크리트 B를 채용하여 모드(B)에 대한 암호키(B) 및 모드(A)에 대한 암호화 키(A)를 생성한다. 구체적으로, 계산은

Key A=h(K시드 ‖ 시크리트 A)

Key B=h(K시드 ‖ 시크리트 B)를 이용하여 수행된다.

여기서 문자 h는 해시 함수를 나타내고, 표현식 a ‖ b는 a 와 b의 비트 결합을 나타낸다.

소스 장치는 전송될 데이터에 추가된 CCI의 값을 판독한다. 만일 CCI 가 복사 금지를 표시하면, 상기 데이터 패킷은 모드(A)에 대한 암호 키(A)에 의해 상기 CCI 와 함께 암호화된다. EMI 모드("11")는 필드(210)에 저장되고, 상기 데이터 패킷은 IEEE 1394 인터페이스를 통해 전송된다. 만일 CCI 가 단일 생성 복사 허용을 표시하면, 상기 데이터는 모드(B)에 대한 암호 키(B)에 의해 상기 CCI 와 함께 암호화되고, EMI 모드("10")는 상기 데이터 패킷의 EMI 모드 필드(210)에 저장되어 패킷화되고, 상기 패킷은 IEEE 1394 인터페이스를 통해 전송된다. 만일 CCI가 무제한 복사를 표시하면, 상기 데이터 패킷은 암호화되지는 않지만 패킷화 된다. 상기 EMI 모드는 필드(210)에 "0"으로써 저장되고 상기 패킷은 전송된다. 그러므로, 전송 장치가 데이터를 암호화하기 위해 사용한 키는 서비스에 따라 결정되는 것이 아니라 상기 데이터에 추가된 EMI 모드에 의해 결정된다.

소스 장치에서와 유사하게, 싱크 장치도 K시드, 시크리트 A, 및 Serect B로부터 키(A 및 B)를 생성시킨다. 수신된 패킷의 EMI는 싱크 장치에 의해 검사되고, 만일 상기 EMI 모드가 모드(A)를 표시하면 상기 데이터는 키(A)를 사용하여 해독되고, 만일 EMI 모드가 모드(B)를 표시하면 상기 데이터는 키(B)를 사용하여 해독된다. 그 다음, 해독된 데이터에 추가된 EMI 모드는 검사된다. 만일 EMI 모드가 복사 금지를 표시하면 상기 데이터는 기록되지 않는다. 만일 EMI 모드가 단일 생성 복사 허용을 표시하면, 상기 EMI 모드는 복사 금지로 바뀌고 상기 데이터와 함께 기록된다. 만일 EMI 모드가 무제한 복사를 표시하면, EMI 모드는 상기 데이터와 함께 기록된다.

는 상기 K시드를 안전하게 싱크 장치로 전송한다. 그러나, 여기에서 사용될 비밀 암호는 시크리트 2T 및 시크리트 2R이다. 위에서 설명한 것처럼, 소스 장치는 키(A 및 B)를 생성시키고 데이터에 추가된 EMI 모드에 따라 독립적으로 데이터를 암호화한다. 상기 소스 장치는 패킷 헤더에 적절히 EMI를 저장하고 그것을 전송한다.

싱크 장치는 소스 장치에서와 유사한 방법으로 키(B)를 생성시킨다. 키(A)가 생성되지 않도록 하기 위해서, 허가 조건에 의해 상기 싱크 장치가 수신에 대한 모드(A)를 사용하는 것이 금지된다고 가정하자. 상기 싱크 장치는 수신된 패킷의 EMI 모드를 검사한다. 만일 EMI 모드가 모드(A)를 표시하면 상기 싱크 장치는 패킷을 취하지 않는다. 만일 EMI 모드가 모드(B)를 표시하면, 상기 싱크 장티는 키(B)에 의해 상기 데이터를 해독하고 상기 패킷을 기록한다. 이 때, 상기 데이터가 모드(B)에서 암호화되었음을 표시하는 정보가 데이터와 함께 기록된다. 만일 EMI 모드가 "0"을 표시하면, 싱크 장치는 데이터를 그대로 기록한다. 이 때, 상기 데이터가 암호화되지 않았음을 표시하는 정보가 상기 데이터와 함께 기록된다.

산업상이용가능성

소스 장치와 비트 스트림 기록(BSR) 장치 사이에서 복사가 방지된 정보를 안전하게 전송하기 위한 방법 및 시스템인 본 발명의 바람직한 실시예가 설명되었다. 본 발명이 특정 실시예로 설명되었을지라도, 본 발명이 그러한 예로써 한정되는 것이 아니고 아래의 청구항에 따라 해석되어야 하는 것은 이해될 수 있을 것이다.

(57)청구의 범위

청구항1

정보 전송 시스템에 있어서,

상기 시스템은 암호화 모드 식별기 (EMI:encryption mode identifier) 코드를 정보 패킷으로 인코딩하고 상기 정보 패킷을 통신 인터페이스를 통해 전송하기 위한 소스 장치 및 상기 통신 인터페이스로부터의 정보 패킷을 수신하기 위한 수신 장치를 포함하되, 상기 소스 장치는

상기 EMI 코드가 제 1 모드를 표시한다면 상기 정보 패킷의 데이터를 암호화하기 위한 제 1 암호화 회로; 및

상기 EMI 코드가 제 2 모드를 표시한다면 제공된 상기 정보 패킷의 상기 데이터를 암호화하기 위한 제 2 암호화 회로를 포함하고, 상기 싱크 장치는

상기 정보 패킷으로부터 상기 EMI 코드를 추출하기 위한 추출기 회로; 및

상기 EMI 코드가 상기 제 2 모드임을 표시하는 상기 추출기 회로에 응답하여 상기 정보 패킷의 상기 데이터를 해독하기 위한 제 2 해독 회로를 포함하되, 여기서 상기 제 1 모드는 상기 정보 패킷이 상기 싱크 장치에 의해서 재생되지 않는다는 것을 표시하는 복사 금지 모드(copy prohibition mode)이고, 상기 제 2 모드는 상기 정보 패킷이 상기 싱크 장치에 의해 일 회 그 이상은 재생되지 않는다는 것을 표시하는 복사 일회 금지 모드(copy once inhibition mode)인, 정보 전송 시스템.

청구항2

제 1항에 있어서, 상기 싱크 장치는 상기 EMI 코드가 상기 제 1 모드임을 표시하는 상기 추출기 회로에 응답하여 상기 정보 패킷의 상기 데이터를 해독하기 위한 제 1 해독 회로를 더 포함하는, 정보 전송 시스템.

청구항3

제 2항에 있어서, 상기 제 1 암호화 회로, 상기 제 2 암호화 회로, 상기 제 1 해독 회로 및 상기 제 2 해독 회로는 동일한 암호 키를 수신하기 위해 결합되는, 정보 전송 시스템.

청구항4

정보 전송 시스템에 있어서,

상기 시스템은 암호화 모드 식별기(EMI:encryption mode identifier) 코드를 정보 패킷으로 인코딩하고 상기 정보 패킷을 통신 인터페이스를 통해 전송하기 위한 소스 장치 및 상기 통신 인터페이스로부터의 정보 패킷을 수신하기 위한 수신 장치를 포함하되, 상기 소스 장치는

만일 상기 EMI 코드가 제 1 모드를 표시하면 제 1 키에 기초하여 상기 정보 패킷의 데이터를 암호화하기 위한 공통 암호화 회로를 포함하되 여기서 상기 공통 암호화 회로는 또한 만일 상기 EMI 코드가 제 2 모드를 표시하면 제 2 키에 기초하여 상기 정보 패킷의 데이터를 암호화하기 위한 회로이고, 상기 싱크 장치는

상기 정보 패킷으로부터 상기 EMI 코드를 추출하기 위한 추출기 회로; 및

상기 EMI 코드가 상기 제 2 모드임을 표시하는 상기 추출기 회로에 응답하여 상기 정보 패킷의 상기 데이터를 상기 제 2 키를 사용

는다는 것을 표시하는 복사 금지 모드이고, 상기 제 2 모드는 상기 정보 패킷이 상기 싱크 장치에 의해 일 회 그 이상은 재생되지 않는다는 것을 표시하는 복사 일회 금지 모드(copy once inhibition mode)인, 정보 전송 시스템.

청구항5

제 1항 또는 제 4항에 있어서, 상기 싱크 장치는 비트 스트림 기록 장치이고, 여기서 상기 싱크 장치는 상기 EMI 코드가 상기 제 2 모드를 표시한다면 상기 정보 패킷을 기록하기 위한 기록 매체를 더 포함하되, 상기 정보 패킷의 상기 EMI 코드는 상기 기록 매체에 기록될 때 상기 싱크 장치에 의해 상기 제 1 모드로 변경되는, 정보 전송 시스템.

청구항6

제 4항에 있어서, 상기 싱크 장치의 상기 공통 해독 회로는 또한 상기 EMI 코드가 상기 제 1 모드임을 표시하는 상기 추출기 회로에 응답하여 상기 정보 패킷의 상기 데이터를 상기 제 1 키를 사용하여 해독하기 위한 회로인, 정보 전송 시스템.

청구항7

제 2항 또는 제 6항에 있어서, 상기 통신 인터페이스는 IEEE 1394 통신 표준에 부합하는 직렬 통신 인터페이스이고 여기서 상기 정보 패킷은 디지털 정보 패킷인, 정보 전송 시스템.

청구항8

제 2항 또는 제 6항에 있어서, 상기 소스 장치는 방송 수신기 장치이고, CCI 정보와 함께 인코딩된 정보 패킷을 수신하고 상기 정보 패킷으로부터 복사 방지 코드를 추출하기 위한 수신기 회로를 더 포함하되, 여기서 상기 싱크 장치는 CCI 정보와 함께 인코딩된 정보 패킷을 처리할 수 없는, 정보 전송 시스템.

청구항9

제 2항 또는 제 6항에 있어서, 상기 정보 패킷은 디지털 오디오/비주얼 프로그램의 부분을 나타내는, 정보 전송 시스템.

청구항10

제 6항에 있어서, 상기 소스 장치 및 상기 싱크 장치는 각각

공통 키에 기초하여 상기 제 1키를 생성시키기 위한 제 1 해시(hash) 회로; 및

상기 공통 키에 기초하여 상기 제 2 키를 생성시키기 위한 제 2 해시 회로를 포함하되, 여기서 상기 공통 키는, 상기 정보 패킷이 상기 싱크 장치에 의해 수신되기 전에 상기 싱크 장치와 상기 소스 장치 사이에서 전송되는, 정보 전송 시스템.

청구항11

복사 방지 모드를 포함하는 정보를 전송하는 방법에 있어서,

소스 장치가 복사 방지 모드를 갖는 정보 패킷을 수신하는 단계;

상기 소스 장치가 암호화 모드 표시기(EMI:encryption mode indicator) 코드를 상기 복사 방지 모드에 따라 상기 정보 패킷의 헤더에 저장하는 단계;

만일 상기 EMI 코드가 제 1 모드를 표시하면, 상기 소스 장치가 상기 정보 패킷의 상기 데이터를 암호화하기 위해 제 1 암호화 메커니즘을 사용하는 단계;

만일 상기 EMI 모드가 제 2 모드를 표시하면, 상기 소스 장치가 상기 정보 패킷의 데이터를 암호화하기 위해 제 2 암호화 메커니즘을 사용하는 단계;

만일 상기 EMI 코드가 제 3 모드를 표시하면, 상기 소스 장치가 상기 정보 패킷의 상기 데이터를 암호화하지 않는 단계; 및

상기 소스 장치가 상기 정보 패킷을 싱크 장치로 전송하는 단계를 포함하는데, 여기서 상기 제 1 모드는 상기 정보 패킷이 상기 싱크 장치에 의해 재생되지 않는다는 것을 표시하는 복사 금지 모드이고, 상기 제 2 모드는 상기 정보 패킷이 상기 싱크 장치에 의해 일 회 그 이상은 재생되지 않는다는 것은 표시하는 복사 일회 금지 모드이며, 상기 제 3 모드는 상기 정보 패킷이 상기 싱크 장치에 의해 자유롭게 재생될 수 있음을 표시하는 무제한 모드(unrestricted mode)인, 복사 방지 모드를 포함하는 정보를 전송하는 방법.

청구항12

제 11항에 있어서, 상기 싱크 장치가 상기 정보 패킷을 수신하고 상기 수신된 정보 패킷으로부터 상기 EMI 코드를 추출하는 단계;

만일 상기 EMI 코드가 상기 제 1 모드라면, 상기 싱크 장치가 제 1 해독 메커니즘을 사용하여 상기 정보 패킷의 상기 데이터를 해독하는 단계;

하는 단계; 및

만일 상기 EMI 코드가 상기 제 3 모드라면, 상기 싱크 장치가 상기 정보 패킷 데이터의 상기 데이터를 해독하지 않는 단계를 더 포함하는, 복사 방지 모드를 포함하는 정보를 전송하는 방법.

청구항13

제 12항에 있어서, 상기 싱크 장치가 상기 EMI 코드를 상기 제 2 모드로부터 상기 제 1 모드로 변화시키고, 새로운 EMI 코드를 상기 정보 패킷에 저장하는 단계; 및

상기 싱크 장치가 상기 정보 패킷을 기록하는 단계를 더 포함하는, 복사 방지 모드를 포함하는 정보를 전송하는 방법.

청구항14

제 12항에 있어서, 상기 소스 장치가 복사 방지 모드를 가지는 정보 패킷을 수신하는 상기 단계는 상기 소스 장치가, 인코딩된 CCI 정보를 가지는 상기 정보 패킷을 상기 복사 방지 모드를 추출하기 위해 변환시키는 단계를 포함하는, 복사 방지 모드를 포함하는 정보를 전송하는 방법.

청구항15

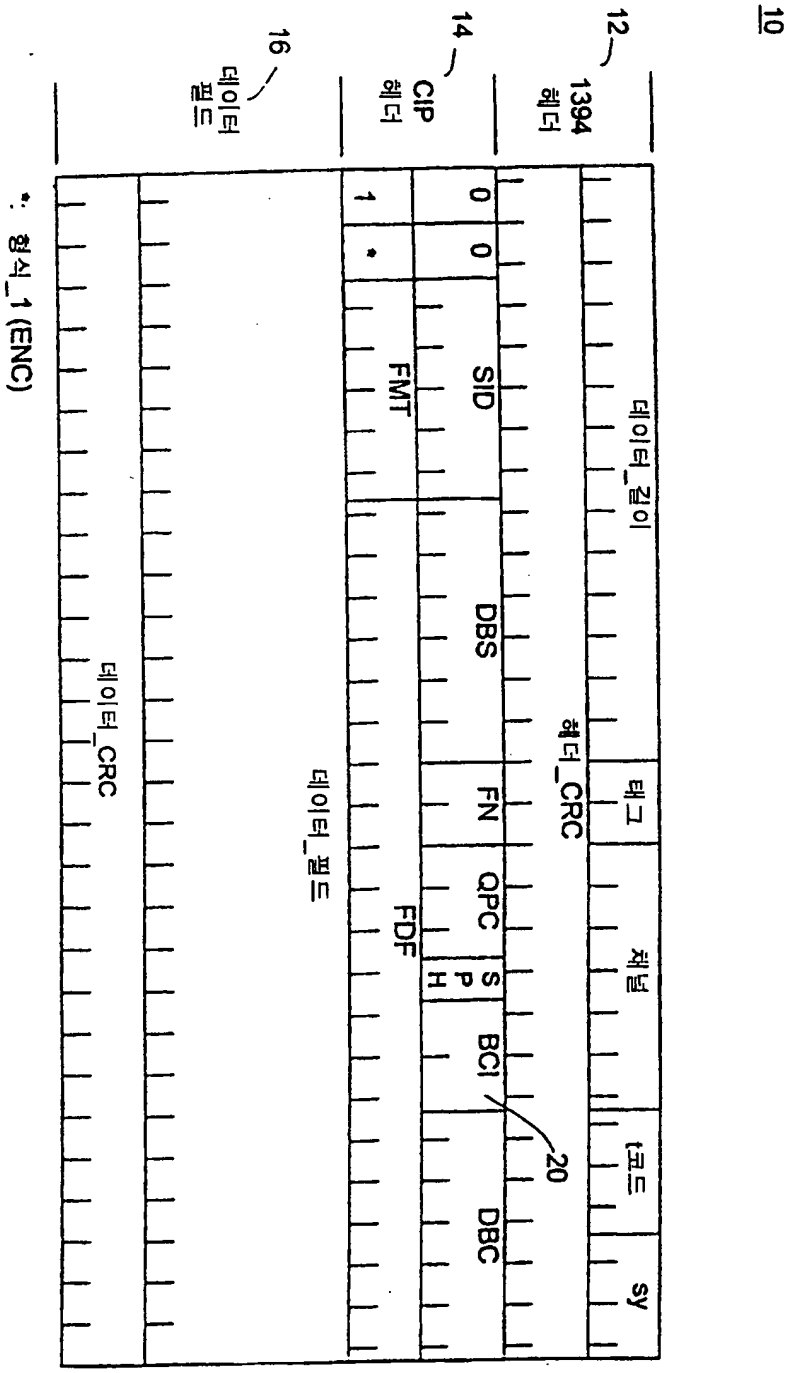
제 12항에 있어서, 상기 정보 패킷은 오디오/비주얼 프로그램의 부분의 디지털 표현인, 복사 방지 모드를 포함하는 정보를 전송하는 방법.

청구항16

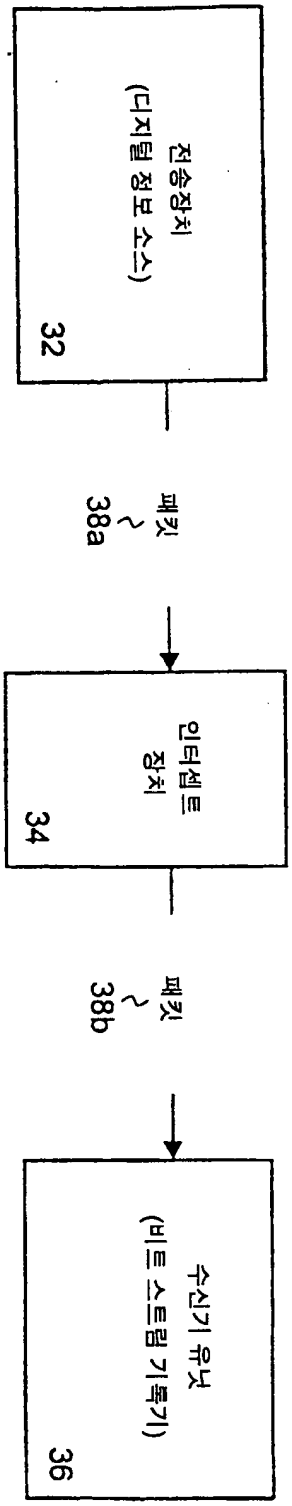
제 12항에 있어서, 상기 소스 장치는 방송 수신기 장치이고, 상기 싱크 장치는 비트 스트림 기록기인, 복사 방지 모드를 포함하는 정보를 전송하는 방법.

도면

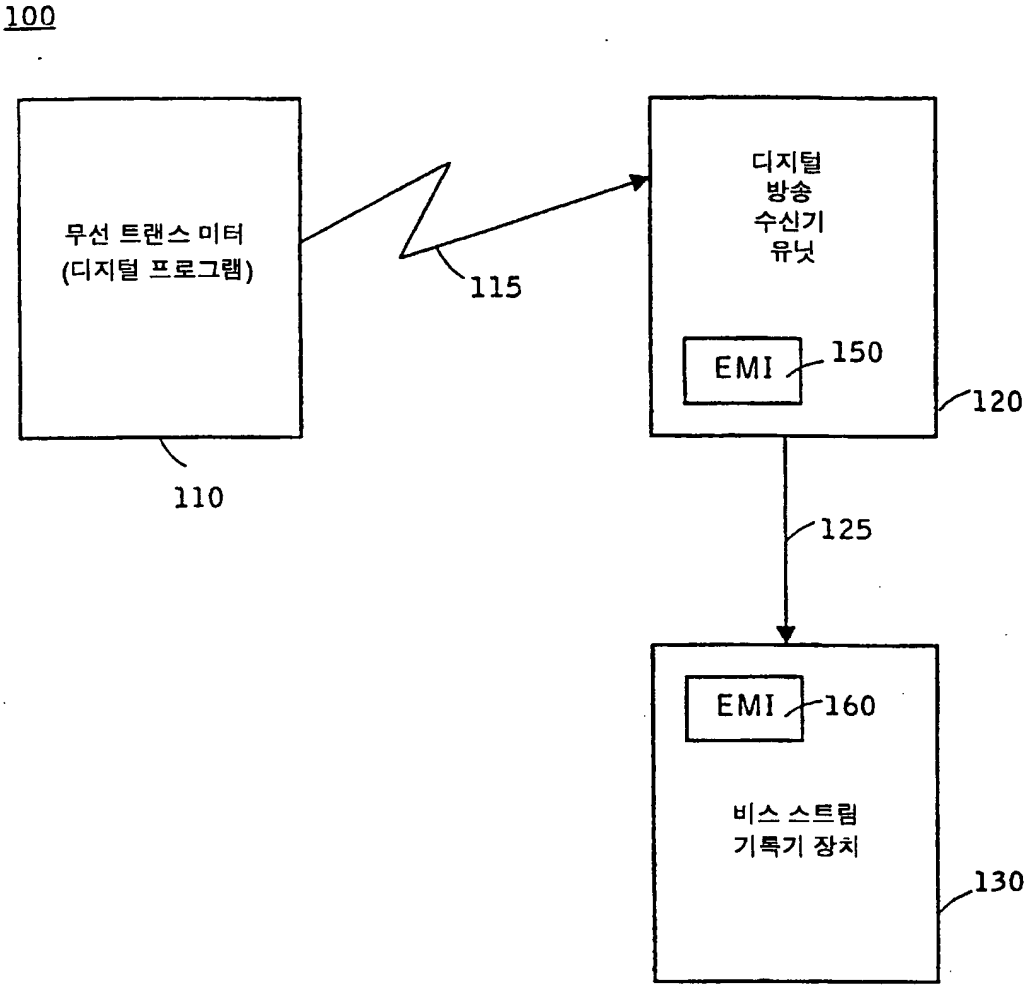
도면1


10
12
1394 헤더
14
CIP 헤더
16
데이터 필드
데이터_길이
태그
채널
t코드
sy
헤더_CRC
0
0
SID
DBS
FN
QPC
SPH
BCI
DBC
20
1
*
FMT
FDF
데이터_필드
데이터_CRC
*: 형식_1 (ENC)

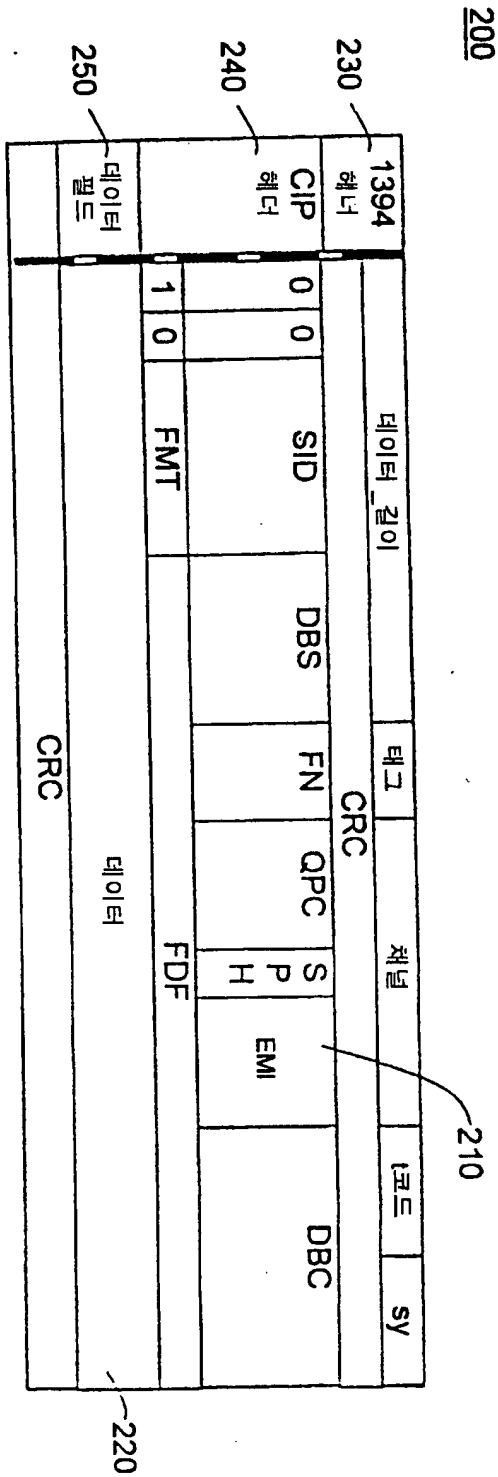
도면2



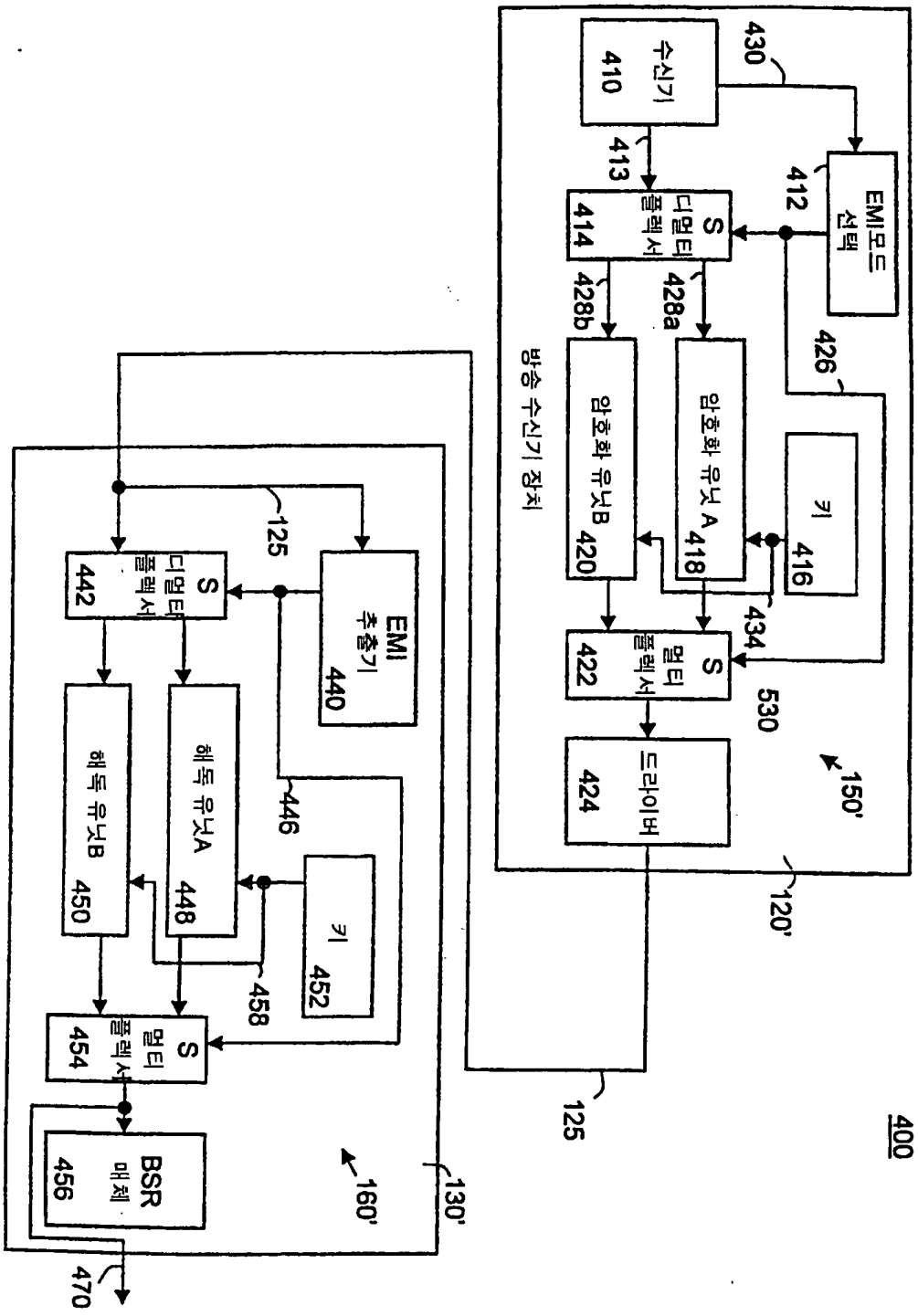
도면3


100
무선 트랜스 미터
(디지털 프로그램)
115
디지털
방송
수신기
유닛
EMI
150
120
110
125
EMI
160
비스 스트림
기록기 장치
130

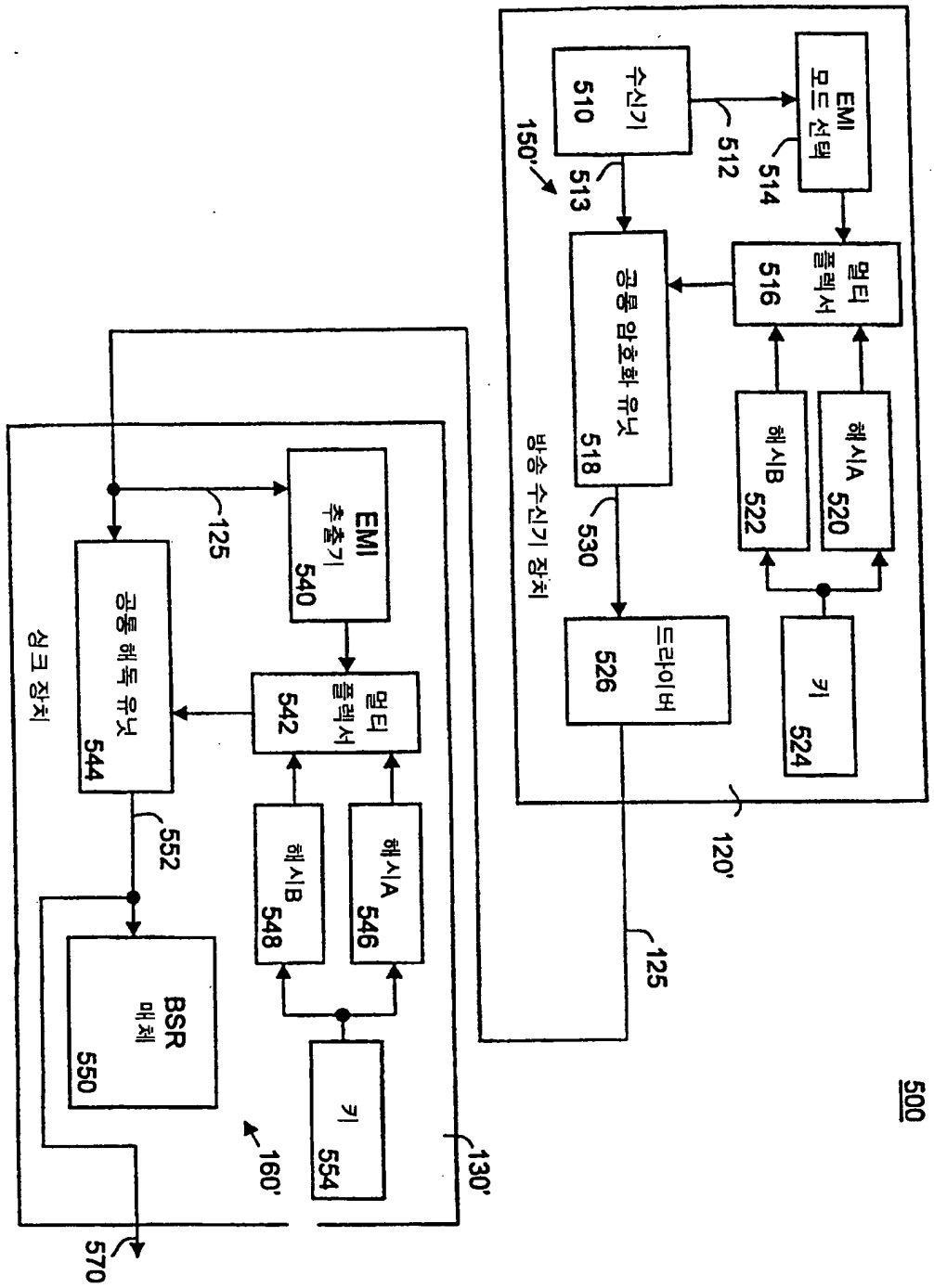
도면4


200
230
240
250
1394 헤더
CIP 헤더
데이터 필드
0
0
1
0
SID
FMT
DBS
FN
QPC
SPH
EMI
FDF
DBC
데이터_길이
태그
채널
t코드
sy
CRC
CRC
데이터
210
220

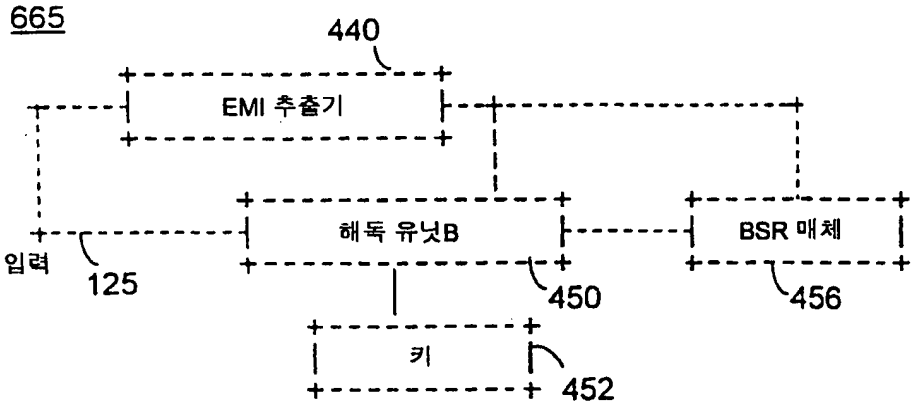
도면5a

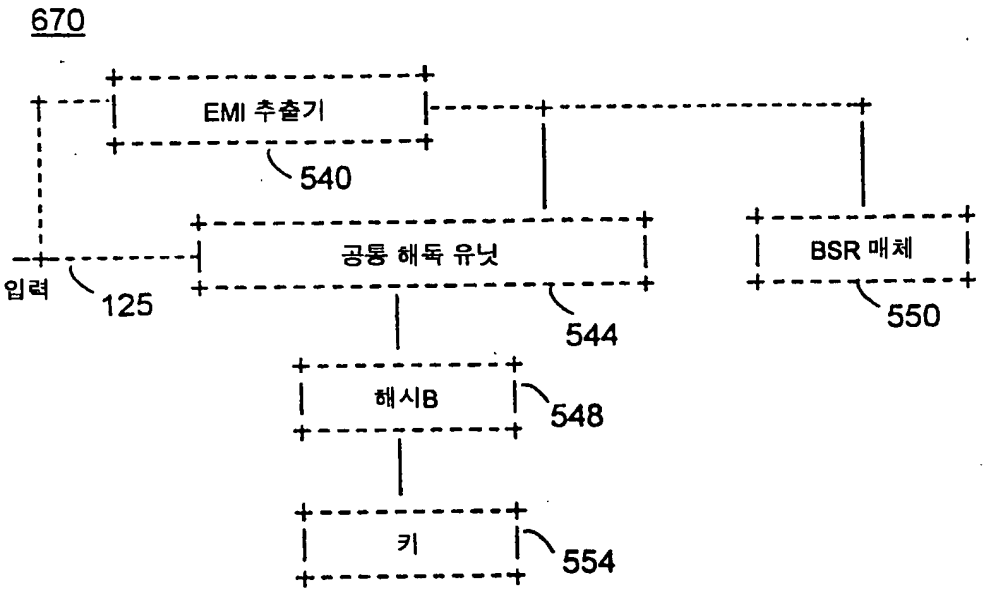

400
방송 수신기 장치
수신기
410
430
EMI모드
선택
412
413
S
디멀티
플렉서
414
428b
428a
426
암호화 유닛B
420
암호화 유닛A
418
키
416
434
S
멀티
플렉서
422
530
드라이버
424
150'
120'
125
125
S
디멀티
플렉서
442
EMI
추출기
440
446
해독 유닛B
450
해독 유닛A
448
키
452
458
S
멀티
플렉서
454
BSR
매체
456
160'
130'
470

도면5b

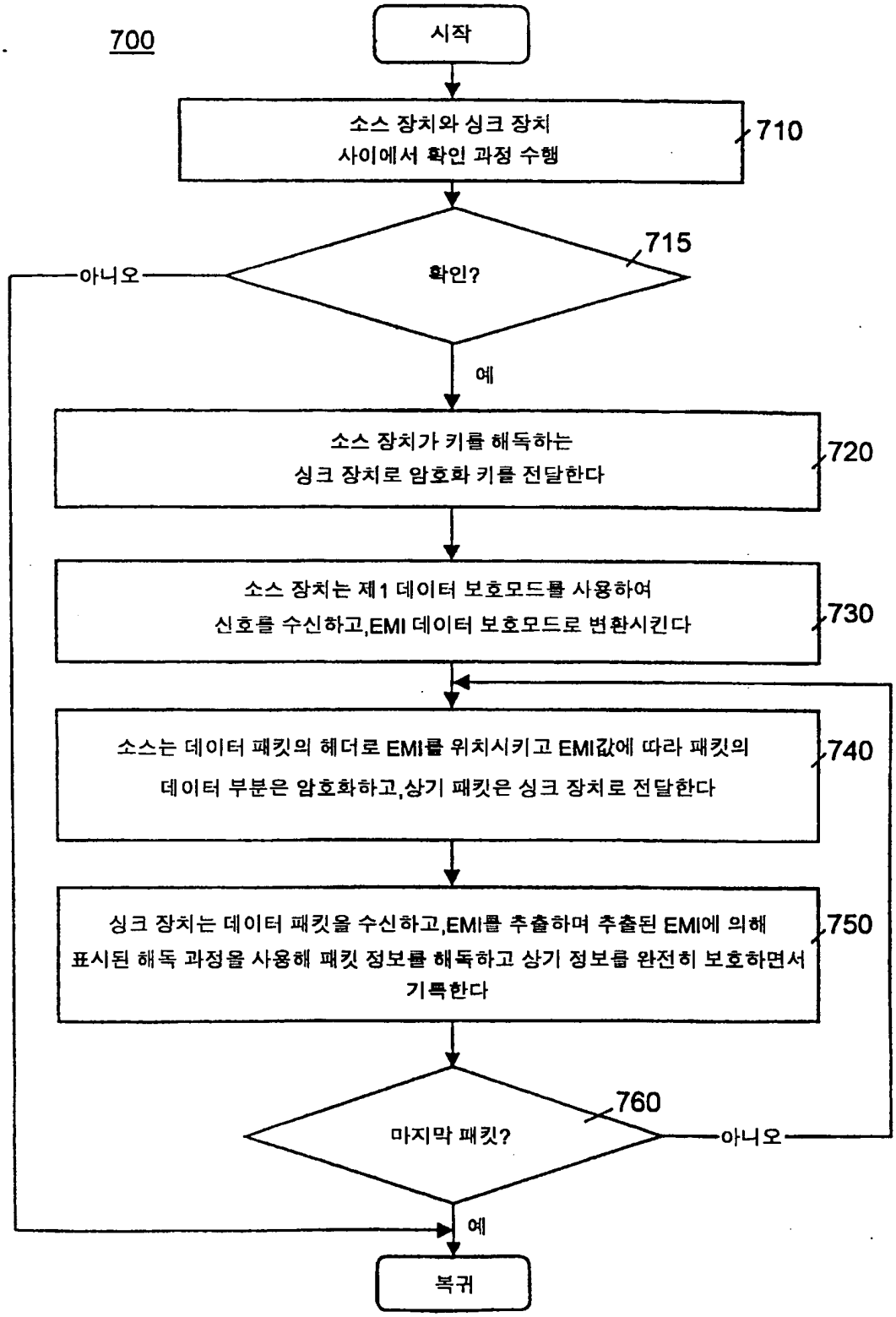

방송 수신기 장치
150'
수신기
510
EMI
모드 선택
512
514
513
멀티
플렉서
516
공통 암호화 유닛
518
530
해시B
522
해시A
520
드라이버
526
키
524
120'
125
싱크 장치
EMI
추출기
540
125
공통 해독 유닛
544
멀티
플렉서
542
552
해시B
548
해시A
546
BSR
매체
550
키
554
160'
130'
570
500

도면6a

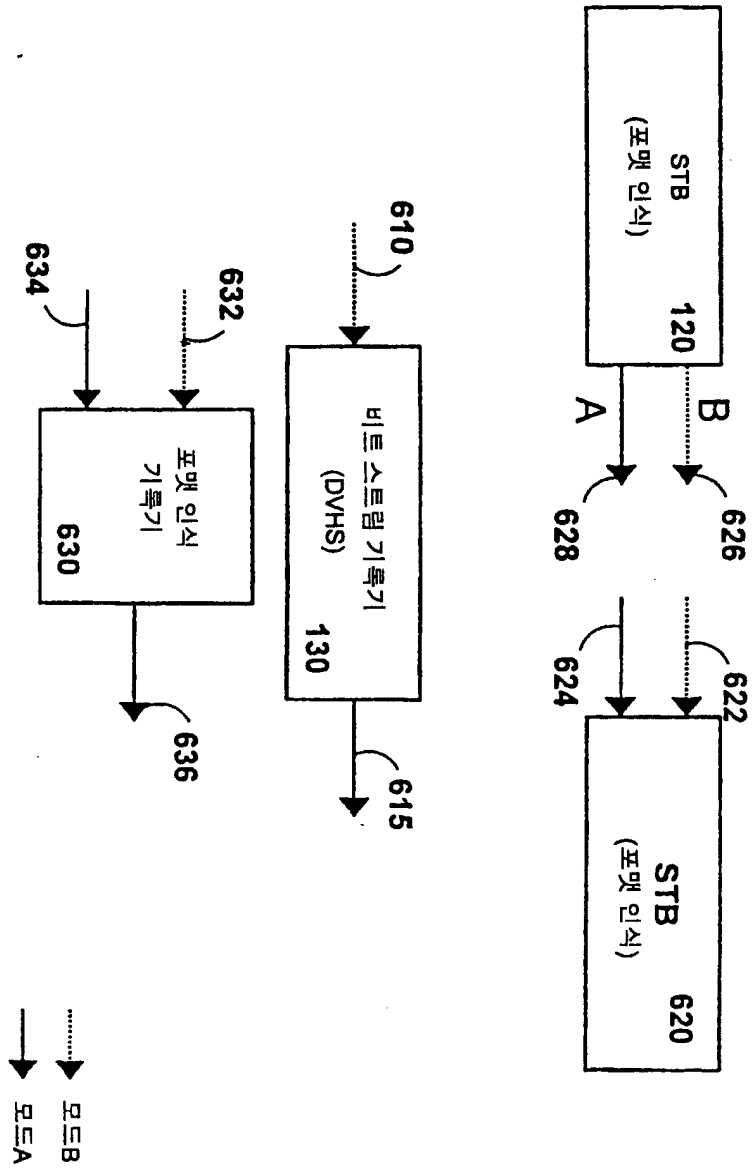

665
440
EMI 추출기
입력
125
해독 유닛B
450
BSR 매체
456
키
452



도면7


700
시작
소스 장치와 싱크 장치
사이에서 확인 과정 수행
710
확인?
715
아니오
예
소스 장치가 키를 해독하는
싱크 장치로 암호화 키를 전달한다
720
소스 장치는 제1 데이터 보호모드를 사용하여
신호를 수신하고,EMI 데이터 보호모드로 변환시킨다
730
소스는 데이터 패킷의 헤더로 EMI를 위치시키고 EMI값에 따라 패킷의
데이터 부분은 암호화하고,상기 패킷은 싱크 장치로 전달한다
740
싱크 장치는 데이터 패킷을 수신하고,EMI를 추출하며 추출된 EMI에 의해
표시된 해독 과정을 사용해 패킷 정보를 해독하고 상기 정보를 완전히 보호하면서
기록한다
750
마지막 패킷?
760
아니오
예
복귀

도면8


STB
(포맷 인식)
120
A
B
628
626
624
622
STB
(포맷 인식)
620
610
비트 스트림 기록기
(DVHS)
130
615
634
632
포맷 인식
기록기
630
636
모드B
모드A

도면9

300

서비스 310	전송 315	시크리트1T
	수신 317	시크리트1R
서비스 320	전송 325	시크리트2T
	수신 327	시크리트2R
서비스 330	전송 335	시크리트3T
	수신 337	시크리트3R
모드A 340		시크리트A
모드B 350		시크리트B